Microsoft System Center 2012 R2

Administering System Center 2012 R2 Service Manager

Microsoft Corporation

Published: November 1, 2013

Authors

Anat Kerry, Bill Anderson, and John Downing

Applies To

System Center 2012 - Service Manager

System Center 2012 Service Pack 1 (SP1) - Service Manager

System Center 2012 R2 Service 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, ActiveX, Active Directory, Bing, Internet Explorer, MSDN, SharePoint, Silverlight, SQL Server, Visual Basic, Visual Studio, Windows, Windows Intune, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. 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 to this guide.

Contents

Administering System Center 2012 - Service Manager ... 8
Using Management Packs in System Center 2012 - Service Manager ... 10
How to Create a Management Pack File ... 11
How to Export a Management Pack ... 12
How to Import a Management Pack ... 13
How to Import the Operations Manager Alert Cube Management Pack ... 14
Using Connectors to Import Data into System Center 2012 - Service Manager ... 15
Effects of Deleting a Connector on Configuration Items ... 16
Importing Data from Active Directory Domain Services ... 16
About Importing Data from Active Directory Domain Services ... 17
How to Create an Active Directory Connector ... 18
How to Synchronize an Active Directory Connector ... 19
How to Disable and Enable an Active Directory Connector ... 20
How to Import Data from Other Domains ... 21
Importing Data and Alerts from System Center Operations Manager ... 22
How to Import Management Packs for System Center Operations Manager Configuration Item Connectors ... 23
How to Create a System Center Operations Manager Connector ... 24
How to Synchronize a System Center Operations Manager Connector ... 28
How to Disable and Enable a System Center Operations Manager Connector ... 28
How to Edit a System Center Operations Manager Connector ... 29
Importing Data from System Center Configuration Manager ... 30
About Importing Data from System Center Configuration Manager ... 31
How to Create a Configuration Manager Connector ... 33
How to Disable and Enable a Configuration Manager Connector ... 35
How to Synchronize a Configuration Manager Connector ... 36
How to Configure a Configuration Manager Connector for an Extended SMS_def.mof File ... 36
Importing Runbooks from System Center Orchestrator 2012 ... 66
How to Create an Orchestrator Connector ... 67
How to Synchronize an Orchestrator Connector ... 68
How to Disable and Enable an Orchestrator Connector ... 69
Importing Data from System Center Virtual Machine Manager ... 69
How to Create a Virtual Machine Manager Connector ... 70
How to Synchronize a Virtual Machine Manager Connector ... 72
How to Disable and Enable a Virtual Machine Manager Connector ... 72
Using a CSV File to Import Data into Service Manager ... 73
About Importing Data from Comma-Separated Files into Service Manager ... 73
How to Import Configuration Items from a CSV File ... 76

Configuration Items in System Center 2012 - Service Manager ... 77
Creating Configuration Items ... 78
About Creating Configuration Items ... 78
How to Manually Create Configuration Items ... 79
How to Create a Service ... 80
How to Create a View for Imported Configuration Items ... 82
Deleting Configuration Items ... 84
How to Initiate the Deletion of a Configuration Item ... 84
How to Delete or Restore a Configuration Item ... 85
Managing Configuration Items ... 86
How to Add, View, or Remove Related Configuration Item Information ... 87
Configuring Incident Management in System Center 2012 - Service Manager ... 88
About Configuring Incident Management in Service Manager ... 89
How to Set File Attachment Limits ... 91
How to Set Parent Incident Options ... 92
How to Set Incident Priority ... 94
How to Set Resolution Time ... 94
How to Set Operations Manager Web Settings ... 95
How to Configure Your Infrastructure for Email Incident Support With Exchange Server 2007 ... 95
How to Configure Your Infrastructure for Email Incident Support with Exchange Server 2010 ... 97
How to Create Incident Templates ... 101
Configuring Service Level Management in System Center 2012 - Service Manager ... 103
About Service Level Management ... 104
How to Create a Calendar Item ... 105
How to Edit a Calendar Item ... 106
How to Create SLA Metrics ... 106
How to Edit SLA Metrics ... 107
How to Modify an SLA Metric View ... 108
How to Create a Service Level Objective ... 108
How to Edit a Service Level Objective ... 109
How to View SLA Information in an Incident Form ... 110
How to Review Incidents with SLA Information ... 111
How to Send SLA Notification Information to the Assigned-To User ... 111
How to Reactivate Incidents with SLA Information ... 112
Configuring Workflows in System Center 2012 - Service Manager ... 113
How to Configure Incident Workflows ... 114
How to View Workflow Success or Failure ... 115
Configuring Change and Activity Management in System Center 2012 - Service Manager ... 116
How to Create Change Request Templates ... 117
How to Create a Manual Activity Template ... 119
How to Configure General Change Settings ... 119

How to Configure General Activity Settings ... 120
How to Configure Change Management Workflows ... 121
How to Configure Activity Management Workflows ... 122
Configuring Release Management in System Center 2012 - Service Manager ... 124
How to Configure Release Management Settings ... 124
How to Configure Release Management Workflows for Notifications ... 125
Configuring Desired Configuration Management to Generate Incidents in System Center 2012 - Service Manager ... 126
How to Configure Desired Configuration Management to Generate Incidents ... 127
Configuring System Center 2012 - Service Manager Notifications ... 128
How to Configure Notification Channels ... 129
How to Create Notification Templates ... 130
How to Subscribe to Notifications ... 133
How to Verify a Notification Configuration ... 136
About Substitution Strings in Notification Templates ... 137
How to Automatically Notify Groups of Users ... 137
Using the Service Catalog in System Center 2012 - Service Manager ... 139
About the Service Catalog ... 140
How to Extend the Service Offering Categories ... 141
How to Create a Service Offering ... 141
How to Create Service Request Templates for New Request Offerings ... 143
How to Create a Request Offering ... 144
How to Publish a Request Offering ... 146
How to Unpublish a Request Offering ... 147
How to Add Request Offerings to Service Offerings ... 147
How to Create a Catalog Item Group ... 148
How to Specify a User Role for Catalog Items ... 149
How to Copy Request Offerings and Service Offerings ... 150
How to Publish a Service Offering ... 151
How to Create and Categorize Catalog Items in Localized Languages ... 152
How to Edit a Service Offering or a Request Offering ... 152
How to Delete a Service Offering or a Request Offering ... 155
About Languages Supported by the Service Catalog ... 156
Using Groups, Queues, and Lists in System Center 2012 - Service Manager ... 158
About Groups, Queues, and Lists ... 159
How to Create a Group ... 161
How to Create a Queue ... 162
How to Edit a Queue ... 163
How to Add a List Item ... 164
Using Runbooks in System Center 2012 - Service Manager ... 164
About Runbooks in Service Manager ... 165
How to Create a Runbook Automation Activity Template ... 166
How to View a Runbook ... 167

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager .. 168
About Chargeback Reports ... 168
Chargeback Report Requirements ... 170
How to Install Chargeback Reports ... 170
How to Create or Modify a Price Sheet ... 173
How to Publish and Unpublish a Price Sheet ... 175
How to Assign or Remove a Default Price Sheet for a Selected Cloud ... 176
How to Override a Default Price Sheet for a Specific VMM User Role ... 177
User Interface Customization in System Center 2012 - Service Manager ... 178
How to Customize a View ... 179
How to Customize a List Item ... 179
How to Customize a Template ... 180
Managing User Roles in System Center 2012 - Service Manager ... 180
About User Roles ... 181
How to Add a Member to a User Role ... 184
How to Create a User Role ... 185
Managing Run As Accounts in System Center 2012 - Service Manager ... 186
How to Change the User Credentials for the Operational Database Account ... 187
How to Change the Password for the Operational Database Account ... 190
How to Change the Workflow Run As Account Credentials ... 191
How to Change the Credentials for SQL Server Analysis Services Account ... 192
How to Change the Credentials for SQL Server Reporting Services Account ... 192
Managing Knowledge Articles in System Center 2012 - Service Manager ... 193
How to Create a Knowledge Article ... 193
How to Search for a Knowledge Article ... 194
Configuring and Using the System Center 2012 - Service Manager Cmdlets for Windows PowerShell ... 196
How to Set Execution Policy ... 197
Getting Started with Service Manager Cmdlets for Windows PowerShell ... 197
How to Import the Data Warehouse Cmdlet Module ... 199
List of the Service Manager Cmdlets ... 199
Managing the Data Warehouse in System Center 2012 - Service Manager ... 207
About Managing the Data Warehouse ... 208
About Data Warehouse Module Deployment ... 211
About Reimporting Previously Removed Management Packs ... 214
Registering Source Systems to the System Center Data Warehouse ... 214
How to Register the System Center Data Warehouse to Operations Manager ... 215
How to Register Configuration Manager With the System Center Data Warehouse to ... 216
How to Register the System Center Data Warehouse to a Service Manager Source ... 217
How to Manage Data Import Jobs for Operations Manager and Configuration Manager. 218
Troubleshooting System Center Data Warehouse Errors ... 219
How to Disable a Data Warehouse Job Schedule ... 227
How to Enable Data Warehouse Job Schedules ... 227

How to View the Status of a Data Warehouse Job ... 228
How to Stop and Start a Data Warehouse Job ... 229
How to Schedule a Data Warehouse Job ... 230
How to Process All Dimensions in the Data Warehouse Using Windows PowerShell Cmdlets ... 231
How to View Data Warehouse Job History ... 232
How to Troubleshoot a Data Warehouse Job ... 232
How to Configure Microsoft SharePoint for Analytics ... 233
Managing the System Center 2012 - Service Manager Self-Service Portal ... 233
How to Configure Concurrent Sessions and Calls ... 234
How to Modify the Self-Service Portal Attachment File Size ... 235
Customizing the Self Service Portal ... 236
How to Update the Portal Title and Image ... 237
How to Add Navigation Links ... 238
How to Update the Portal Theme ... 239
How to Add a Portal Announcement Page ... 239
How to Modify the Help Article Web Part ... 240
How to Modify a Master Page File ... 240
How to Select the Self Service Portal Language ... 241
Enabling Tracing and Debugging for the Self Service Portal ... 242
Using Service Manager Tasks to Troubleshoot Computer Problems ... 243
How to Create a Task ... 243
How to Run a Task from an Incident View ... 245
To Configure System Center 2012 - Service Manager CEIP Settings ... 245
Appendix A - List of User Role Profiles in System Center 2012 - Service Manager ... 246
Appendix B - Mapping Active Directory Domain Services Attributes to Properties in System Center 2012 - Service Manager ... 265
Appendix C - Mapping System Center 2012 - Service Manager Properties to Configuration Manager Database Views ... 269
Appendix D - System Center 2012 - Service Manager Registry Keys ... 281

Administering System Center 2012 - Service Manager

Welcome to the Administrator's Guide for Microsoft System Center 2012 – Service Manager. This guide describes concepts that are important to Service Manager administrators, and it includes procedures that Service Manager administrators must perform to configure Service Manager. These procedures are typically performed one time after Service Manager is deployed. The procedures in this guide help you configure Service Manager to match the policies and requirements defined by your organization.

Administrator's Guide Topics

- Using Management Packs in System Center 2012 - Service Manager

  Provides information about how to create, import, and export management packs in Service Manager.
- Using Connectors to Import Data into System Center 2012 - Service Manager

  Describes how to import data into Service Manager by using connectors.
- Configuration Items in System Center 2012 - Service Manager

  Describes how to manage configuration items in Service Manager.
- Configuring Incident Management in System Center 2012 - Service Manager

  Describes how to set configuration settings that streamline the creation of incidents in Service Manager.
- Configuring Service Level Management in System Center 2012 - Service Manager

  Provides an overview of how to configure service-level management in Service Manager.
- Configuring Workflows in System Center 2012 - Service Manager

  Describes how to create and use workflows in Service Manager.
- Configuring Change and Activity Management in System Center 2012 - Service Manager

  Describes how to streamline change and activity management in Service Manager.
- Configuring Release Management in System Center 2012 - Service Manager

  Describes how to configure settings and workflows for release management.
- Configuring Desired Configuration Management to Generate Incidents in System Center 2012 - Service Manager

  Describes how to configure Service Manager to create incidents based on desired configuration management reports from System Center Configuration Manager 2007.
- Configuring System Center 2012 - Service Manager Notifications

  Describes how to configure notifications in Service Manager.
- Using the Service Catalog in System Center 2012 - Service Manager

Provides an overview of how to use the service catalog in Service Manager.

- Using Groups, Queues, and Lists in System Center 2012 - Service Manager

  Describes how to use groups to manage configuration items, use queues to manage work items, and use lists to customize forms in Service Manager.

- Using Runbooks in System Center 2012 - Service Manager

  Describes how to use runbooks in Service Manager and System Center 2012 - Orchestrator to automate procedures.

- Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

  Describes how to install and configure chargeback reports.

- User Interface Customization in System Center 2012 - Service Manager

  Describes how to use unsealed management packs to edit the properties of views, list items, or templates.

- Managing User Roles in System Center 2012 - Service Manager

  Provides an overview of user roles and describes how to use user roles to define a scope of activities that can be performed in Service Manager.

- Managing Run As Accounts in System Center 2012 - Service Manager

  Describes how to change the Operational System and Workflow Run As accounts.

- Managing Knowledge Articles in System Center 2012 - Service Manager

  Describes how to create and search for knowledge articles.

- Configuring and Using the System Center 2012 - Service Manager Cmdlets for Windows PowerShell

  Describes how to use the Service Manager cmdlets for Windows PowerShell.

- Managing the Data Warehouse in System Center 2012 - Service Manager

  Describes how to view, schedule, and troubleshoot extract, transform, and load (ETL) jobs.

- Managing the System Center 2012 - Service Manager Self-Service Portal

  Describes how to customize the portal home page, add navigational links, and how to configure concurrent sessions and calls in the Self-Service Portal.

- Using Service Manager Tasks to Troubleshoot Computer Problems

  Describes how to use tasks to troubleshoot computer problems.

- To Configure System Center 2012 - Service Manager CEIP Settings

  Describes how to configure Customer Experience Improvement Program (CEIP) settings in Service Manager.

- Appendix A - List of User Role Profiles in System Center 2012 - Service Manager

  Lists the user role profiles.

- Appendix B - Mapping Active Directory Domain Services Attributes to Properties in System Center 2012 - Service Manager

  Describes the mapping of data that is imported by Active Directory Connector to Service Manager properties.

- Appendix C - Mapping System Center 2012 - Service Manager Properties to Configuration Manager Database Views

  Describes the mapping of data that is imported by Configuration Manager Connector to Service Manager properties.
- Appendix D - System Center 2012 - Service Manager Registry Keys

  Describes registry settings for System Center 2012 – Service Manager.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

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.

Using Management Packs in System Center 2012 - Service Manager

There are two types of management packs: sealed management packs and unsealed management packs. A sealed management pack cannot be modified, but an unsealed management pack can be modified.

Unsealed management packs are used to extend System Center 2012 – Service Manager with the information that you must have to implement all or part of a service management process. You can use unsealed management packs to store the custom objects that you create. For example, you can store the objects you create during your testing or evaluation process in an unsealed management pack. Then, you can export that unsealed management pack to a file and then import the file to another environment, such as a production environment. You can also import the same management pack into multiple environments to ensure configuration consistency across Service Manager deployments, and to increase efficiency.

Note

Only unsealed management packs can be re-imported.

An unsealed management pack is an .xml file that contains classes, workflows, views, forms, reports, and knowledge articles. Items such as groups, queues, tasks, templates, connectors, and list items are stored in a management pack, but items such as incidents, change requests, computers, and other instances of classes are not stored in a management pack.

By default, Service Manager contains several pre-imported, sealed management packs that enable core Service Manager features, such as incident management and change management. Also, by default, Service Manager contains the **Default Management Pack** management pack, in

which you can store new items that you create. Additionally, Service Manager contains several pre-imported, unsealed management packs that enable optional features. You can delete unsealed management packs, which might result in the loss of some views, rules, or lists. However, the removal of these optional features will not prevent Service Manager from functioning. You should consider exporting a management pack before you delete it. You can import the management pack later if you need the optional features in a management pack that you deleted.

To use a management pack, import it into Service Manager. The management pack is stored in a .xml, .mp, or a .mpb file that you can import by using the Service Manager console.

For more information about management packs key concepts, management packs best practices and other management packs related topics, see Management Packs: Working with Management Packs.

Using Management Packs Topics

- How to Create a Management Pack File

  Describes how to create a management pack file.
- How to Export a Management Pack

  Describes how to export a management pack.
- How to Import a Management Pack

  Describes how to import a management pack by using the Service Manager console.
- How to Import the Operations Manager Alert Cube Management Pack

  Describes how to import the Operations Manager Alert Cube management pack manually.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Create a Management Pack File

You can use the following procedures to create a management pack file in System Center 2012 – Service Manager. After you create the management pack file, you can use it to store objects that you create.

For more information about how to create and customize management packs, see Management Packs: Working with Management Packs.

To create a management pack file

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Management**

Packs.

3. In the **Tasks** pane, under **Management Packs**, click **Create Management Pack**.
4. In the **Create Management Pack** dialog box, enter a name, such as **Sample Management Pack**, and then enter a description for the new management pack. Click **OK**.

To validate the creation of a management pack file

- In the Service Manager console, open the **Management Packs** view, and verify that the new management pack appears in the **Management Packs** pane.

You can use Windows PowerShell commands to complete these tasks, as follows:

- For information about how to use Windows PowerShell to create a new management pack, see New-SCSMManagementPack.
- For information about how to use Windows PowerShell to seal a management pack, preventing it from being modified, see Protect-SCSMManagementPack.
- For information about how to use Windows PowerShell to remove management packs, see Remove-SCSMManagementPack.

How to Export a Management Pack

After you create a management pack in System Center 2012 – Service Manager, you can export the unsealed management pack as a file to back up any customizations in the management pack. The exported management pack is a valid XML-formatted file. After you export an unsealed management pack, you can later import it to restore the objects that the management pack contains.

When you export a sealed management pack, from the Service Manager console or by using the Windows PowerShell cmdlet Export-SCSMManagementPack, Service Manager generates an equivalent, unsealed management pack and stores it as a .XML file on the hard drive. You can then edit this management pack file to increase the version of the management pack, and re-seal it so it can be re-imported into Service Manager.

Use the following procedures to export an unsealed management pack and then validate the export.

To export a management pack

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Management Packs**.
3. In the **Management Packs** pane, select the management pack that you want to export.
4. In the **Tasks** pane, under the name of the management pack that you want to export, click **Export**.
5. In the **Browse For Folder** dialog box, select a location for the file, and then click **OK**.

Note

You cannot change the default name of the management pack file.

To validate the export of a management pack

- In Windows Explorer, ensure that you can locate the management pack file.

You can use Windows PowerShell commands to complete this task. For information about how to use Windows PowerShell to export a management pack as a valid XML-formatted file that you can later import into Service Manager or Operations Manager, see Export-SCSMManagementPack.

See Also

How to Import a Management Pack

How to Import a Management Pack

Before you can use a management pack in System Center 2012 – Service Manager, you must import the management pack by using one of the following methods:

- Use the Service Manager console, as described in this topic.
- Use the **Import-SCSMManagementPack** cmdlet from the Service Manager module for Windows PowerShell. For more information about this cmdlet, see Import-SCSMManagementPack.

When you reimport a sealed management pack, the version of the new management pack must be greater than the version of the initial management pack. The imported, sealed management pack must pass backward-compatibility verification, and then the objects of the new management pack and the objects of the initial management pack are merged. When you reimport an unsealed management pack, the objects from the new management pack overwrite the objects from the initial management pack.

If the management pack that you want to import depends on other management packs, multi-select the dependent management packs and import them in a single operation. Service Manager will import the management packs in the correct dependency order.

Use the following procedure to import a single management pack, or a management pack bundle (.mpb file name extension), by using the Service Manager console. For more information about working with custom management packs, sealed and unsealed management packs, and bundling management packs, see the Authoring Guide for System Center 2012 – Service Manager.

To import a management pack by using the Service Manager console

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Management Packs**.
3. In the **Tasks** pane, under **Management Packs**, click **Import**.

4. In the **Select Management Packs to Import** dialog box, select the management pack file, and then click **Open**.
5. In the **Import Management Packs** dialog box, click **Add**.
6. After you have added all the management packs that you want to import, click **Import**, and then click **OK**.

To validate the import of a management pack

- In the Service Manager console, select the **Management Packs** view, and ensure that the intended management packs appear in the **Management Packs** list.

You can use Windows PowerShell commands to complete these and other related tasks, as follows:

- For information about how to use Windows PowerShell to import a management pack, see Import-SCSMManagementPack.
- For information about how to use Windows PowerShell to test the validity of a management pack, see Test-SCSMManagementPack.
- For information about how to use Windows PowerShell to retrieve objects that represent management packs that have been imported, see Get-SCSMManagementPack.

How to Import the Operations Manager Alert Cube Management Pack

By default, System Center 2012 – Service Manager does not automatically import the System Center Alert Management Cube management pack when you register Operations Manager as a data source.

Instead you must manually create a data source for Operations Manager. For more information, see How to Register the System Center Data Warehouse to Operations Manager. Afterward, use the following procedure to import the management pack.

To import the Operations Manager alert cube management pack

1. In the Service Manager console, click **Data Warehouse**, click **Management Packs**, and confirm that **System Center Datawarehouse Operations Manager Library** is listed.
2. On the Data Warehouse Management Server, type the following Windows PowerShell commands to manually import the management pack. (This example assumes that Service Manager is on drive C and that you installed Service Manager using the default path).

```
cd 'C:\Program Files\Microsoft System Center 2012\Service
Manager'
cd.\PowerShell
Import-Module .\System.Center.Service.Manager.psd1
Import-SCSMManagementPack ..\AlertCube.mpb
```

Using Connectors to Import Data into System Center 2012 - Service Manager

You can use System Center 2012 – Service Manager connectors to import data as configuration items from Active Directory Domain Services (AD DS), System Center Configuration Manager, System Center 2012 - Orchestrator, System Center 2012 – Virtual Machine Manager (VMM), and System Center Operations Manager. In addition, you can import alerts from Operations Manager, and you can configure these alerts to automatically generate incidents in Service Manager. You can also import data from comma-separated value (CSV) files into the Service Manager database.

Using Connectors to Import Data Topics

- Effects of Deleting a Connector on Configuration Items

  Describes the effects of deleting a connector.
- Importing Data from Active Directory Domain Services

  Describes how to create, synchronize, and disable or enable an Active Directory connector.
- Importing Data and Alerts from System Center Operations Manager

  Describes how to create, synchronize, edit, disable or enable an Operations Manager alert or configuration item (CI) connector.
- Importing Data from System Center Configuration Manager

  Describes how to create a connector to System Center Configuration Manager and how to customize configuration management to extend the hardware information that is collected.
- Importing Runbooks from System Center Orchestrator 2012

  Describes how to import runbooks from System Center Orchestrator.
- Importing Data from System Center Virtual Machine Manager

  Describes how to import VMM objects into the Service Manager database.
- Using a CSV File to Import Data into Service Manager

  Describes how to import data into Service Manager by using a CSV file.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

Effects of Deleting a Connector on Configuration Items

Many of the configuration items that are found in the System Center 2012 – Service Manager database are the result of the data that is imported by using connectors. Therefore, if a connector is deleted, the configuration items that are associated with that connector will also be deleted, except where the configuration item is related to an active incident or change request. If more than one connector defines a configuration item, the configuration item will be deleted when all of the contributing connectors are deleted.

If you are creating a new connector to replace an existing connector, create the new connector first, and then synchronize the new connector before deleting the old connector.

Tip

You can use a Windows PowerShell command to remove a connector from Service Manager. For more information, see Remove-SCSMConnector.

Importing Data from Active Directory Domain Services

This section provides an overview of using a connector to import data from Active Directory Domain Services (AD DS) into System Center 2012 – Service Manager. This section also describes how to create, synchronize, and enable or disable an Active Directory connector.

Importing Data from Active Directory Domain Services Topics

- About Importing Data from Active Directory Domain Services

  Provides an overview of how to use a connector to import data from AD DS.
- How to Create an Active Directory Connector

  Describes how to create an Active Directory connector.
- How to Synchronize an Active Directory Connector

  Describes how to synchronize the data in AD DS with the Service Manager database.
- How to Disable and Enable an Active Directory Connector

  Describes how to enable or disable an Active Directory connector.
- How to Import Data from Other Domains

  Describes how to import data from domains other than the domain in which Service Manager resides.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Importing Data from Active Directory Domain Services

The Service Manager database in System Center 2012 – Service Manager contains information about your enterprise, and it is used by all the parts of your service management structure. You can use an Active Directory connector to add users, groups, printers, and computers (and only these object types) as configuration items into the Service Manager database.

Note

If the same user name exists in two different organizational units (OUs) within the Active Directory domain, Service Manager cannot import both user accounts, and an event is logged in the System Center Operations Manager application log.

In addition, when you configure an Active Directory connector to import data from an Active Directory group, you can select an option to automatically add users from the Active Directory group. When they are selected, any users that are added to the Active Directory group will be automatically added to the Service Manager database. If those users are removed from the Active Directory group, they will remain in the Service Manager database; however, they will reside in the Deleted Items group.

When you have created an Active Directory connector, **Select objects** in the connector cannot be updated. Instead, you create security groups in Active Directory that map to User Roles in Service Manager. For example, you can create a Security Group in Active Directory Domain Services (AD DS), named Incident Resolvers. In Service Manager, you can assign this security group to the Incident Resolvers user role. When you create the Active Directory connector and you select **Automatically add users of AD Groups imported by this connector**, when a user who is a member of the Incident Resolvers security group starts the Service Manager console, they will be granted Incident Resolver rights and permissions.

If you are importing data from several OUs or subdomains, you have the option of creating a Lightweight Directory Access Protocol (LDAP) query that specifies computers, printers, users, or user groups to import with the connector. For example, an LDAP filter of all objects that are in either Dallas or Austin and that have the first name of John looks like `(&(givenName=John)(|(l=Dallas) (l=Austin)))`. You can test your queries, and all errors must be corrected before you can configure the Active Directory connector. For more information about LDAP queries, see Search Filter Syntax.

If you must later perform maintenance operations on the Service Manager database, you can temporarily disable the connector and suspend the importation of data. Later, you can resume the importation of data by re-enabling the connector.

When you import a large number of users from AD DS) or from System Center Configuration Manager, CPU utilization might increase to 100 percent. You will notice this on one core of the CPU. For example, if you import 20,000 users, CPU utilization might remain high for up to an hour. You can mitigate this issue by creating connectors and importing the users into Service Manager before you deploy the product in your enterprise and by scheduling connector synchronization during off hours. Installing Service Manager on a computer that has a multi-core CPU also minimizes the impact of importing a large number of users.

See Also

How to Create an Active Directory Connector

How to Disable and Enable an Active Directory Connector

How to Synchronize an Active Directory Connector

How to Import Data from Other Domains

Appendix B - Mapping Active Directory Domain Services Attributes to Properties in System Center 2012 - Service Manager

How to Create an Active Directory Connector

You can use the following procedures in System Center 2012 – Service Manager to create, validate, and confirm the status of an Active Directory connector to import objects from Active Directory Domain Services (AD DS).

To create an Active Directory connector and to import objects from AD DS

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Active Directory Connector**.
4. Complete these steps in the Active Directory Connector Wizard:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that the **Enable this connector** check box is selected, and then click **Next**.
   c. On the **Domain or organizational unit** page, select **Use the domain: <domain name>**. Or, select **Let me choose the domain or OU**, and then click **Browse** to choose a domain or an organizational unit (OU) in your environment.
   d. In the **Credentials** area, click **New**.
   e. In the **Run As Account** dialog box, in the **Display name** box, enter a name for the Run As account. In the **Account** list, select **Windows Account**. Enter the credentials for an account that has rights to read from AD DS, and then click **OK**. On the **Domain or organizational unit** page, click **Test Connection**.

      Note
      Special characters (such as the ampersand [&]) in the **User Name** box are not supported.

   f. In the **Test Connection** dialog box, make sure that **The connection to the server was successful** is displayed, and then click **OK**. On the **Domain or organizational unit** page, click **Next**.
   g. On the **Select objects**, do the following:
      i. Select **All computers, printers, users, and user groups** to import all items or,
      ii. Select **Select individual computers, printers, users or user groups** to import only the selected items or,

iii. Select **Provide LDAP query filters for computers, printers, users, or user groups** if you want to create your own Lightweight Directory Access Protocol (LDAP) query.

If you want new users that are added to any groups you import to be added automatically to Service Manager, select **Automatically add users of AD Groups imported by this connector**, and then click **Next**.

h. On the **Summary** page, make sure that the settings are correct, and then click **Create**.

i. On the **Completion** page, make sure that you receive the following confirmation message:

"Active Directory connector successfully created."

Then, click **Close**.

Note

Depending on the amount of data that is imported, you might have to wait for the import to be completed.

To validate the creation of an Active Directory connector

1. In the **Connectors** pane, locate the Active Directory connector that you created. You might have to wait for a minute before the connector appears.
2. In the **Connectors** pane, review the **Status** column for a status of **Finished Success**.
3. In the **Configuration Items** pane, expand **Configuration Items**. Expand **Computers** and **All Windows Computers**, and verify that the intended computers from AD DS appear in the **All Windows Computers** pane. Expand **Printers**, expand **All Printers**, and then verify that the intended printers from AD DS appear in the **All Printers** pane.
4. In the Service Manager console, click **Configuration Items**. In the **Configuration Items** pane, click **Users**, and then verify that the intended users and user groups from AD DS appear in the **Users** pane.

To confirm the status of an Active Directory connector

- View the columns in the **Connector** pane; the columns contain information about the start time, the finish time, the status, and the percentage of imported configuration items.

You can use a Windows PowerShell command to create a new Service Manager Active Directory connector. For information about how to use Windows PowerShell to create a new Service Manager Active Directory connector, see New-SCADConnector.

How to Synchronize an Active Directory Connector

To ensure that the System Center 2012 – Service Manager database is up to date, the Active Directory connector synchronizes with Active Directory Domain Services (AD DS) every hour

after the initial synchronization. However, you can use the following procedure to manually synchronize the connector and validate that it is synchronized.

To manually synchronize an Active Directory connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Active Directory connector that you want to synchronize.
4. In the **Tasks** pane, under the name of the connector, click **Synchronize Now**.

   Note
   Depending on the amount of data that is imported, you might have to wait for the import to be completed.

To validate that an Active Directory connector synchronized

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Printers**, and then click **All Printers**. Verify that any new printers in AD DS appear in the middle pane.
3. Expand **Computers**, and then click **All Windows Computers**. Verify that any new computers in AD DS appear in the middle pane.
4. In the Service Manager console, click **Configuration Items**.
5. In the **Configuration Items** pane, click **Users**. Verify that any new users and groups in AD DS appear in the middle pane.

How to Disable and Enable an Active Directory Connector

You can use the following procedure to disable or enable an Active Directory connector in System Center 2012 – Service Manager and validate its change in status.

To disable an Active Directory connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Active Directory connector that you want to disable.
4. In the **Tasks** pane, under the connector name, click **Disable**.
5. In the **Disable Connector** dialog box, click **OK**.

To enable an Active Directory connector

1. In the Service Manager console, click **Administration**, and then click **Connectors**.
2. In the **Connectors** pane, select the Active Directory connector that you want to enable.

3. In the **Tasks** pane, under the connector name, click **Enable**.
4. In the **Enable Connector** dialog box, click **OK**.

To validate the status change of an Active Directory connector

1. After you enable or disable an Active Directory connector, wait for about 30 seconds. Then, in the Service Manager console, click **Administration**, and then click **Connectors**.
2. In the middle pane, locate the connector for which you have changed status, and then verify the value in the **Enabled** column.

You can use Windows PowerShell commands to complete these tasks and other related tasks, as follows:

- For information about how to use Windows PowerShell to start a Service Manager connector, see Start-SCSMConnector.
- For information about how to use Windows PowerShell to retrieve connectors that are defined in Service Manager and view their status, see Get-SCSMConnector.
- For information about how to use Windows PowerShell to update properties of a Service Manager connector, see Update-SCSMConnector.

How to Import Data from Other Domains

You can import data from domains other than the domain in which System Center 2012 – Service Manager resides. For example, Service Manager is installed in domain A (where the fully qualified domain name [FQDN] is a.woodgrove.com), and you want to import data from domain B (where the FQDN is b.woodgrovetest.net). In this scenario, you must think about how to specify the data source path and how to specify the Run As account.

In domain B, either identify an existing service account or create a new one for this purpose. This service account must be a domain account and must be able to read from Active Directory Domain Services.

Next, in Service Manager, create a new Active Directory connector in the Active Directory Connector Wizard. Follow these steps on the **Domain or organizational unit** page.

To specify the data source path and Run As account

1. Use the appropriate method, according to where the domains are located:
   - If the two domains are in the same forest, in the **Server Information** area, select **Let me choose the domain or OU**, and then click **Browse** to select the domain and organizational unit (OU).
   - If the two domains are in different forests, in the **Server Information** area, select **Let me choose the domain or OU**, and then type the domain and OU in the box. For example, type **LDAP://b.woodgrovetest.net/OU=<OU Name>,DC=b,DC=woodgrovetest,DC=net**.
2. In the **Credentials** area, click **New**.

3. In the **Run As Account** dialog box, in the **User name**, **Password**, and **Domain** boxes, type the credentials for the service account from the b.woodgrovetest.net domain.

   Note
   If the two domains are in different forests, you must type the domain name in the **User name** box. For example, type **b.woodgrovetest.net\<user name>**.

Importing Data and Alerts from System Center Operations Manager

If your organization uses System Center Operations Manager to monitor systems in your enterprise, the agents that are deployed gather information about configuration items that are discovered, and, as problems are detected, System Center Operations Manager generates alerts. Two connectors for Operations Manager are available in System Center 2012 – Service Manager: the configuration item (CI) connector that imports objects that are discovered by Operations Manager into the Service Manager database, and an alert connector that can create incidents based on alerts.

System Center Operations Manager collects information about many different types of objects, such as hard disk drives and Web sites. To import objects that are discovered by Operations Manager, Service Manager requires a list of class definitions for these objects; the list of definitions is in the System Center Operations Manager management packs. Therefore, you must import some System Center Operations Manager management packs into Service Manager. When you install Service Manager, a set of System Center Operations Manager management packs for common objects and the required Windows PowerShell scripts are copied to your Service Manager installation folder. For more information, see How to Import Management Packs for System Center Operations Manager Configuration Item Connectors. If you have installed additional management packs in Operations Manager, and you want to add the data from those additional management packs to Service Manager, you can modify the configuration item (CI) connector to add the additional management packs. For more information, see How to Edit a System Center Operations Manager Connector.

The Windows Azure management pack for Operations Manager 2007 R2 is supported in this release of Service Manager. This means that if an alert from Windows Azure is generated in Operations Manager 2007 R2, Service Manager will recognize the alert and an incident can be created.

Importing Data and Alerts from Operations Manager Topics

- How to Import Management Packs for System Center Operations Manager Configuration Item Connectors

  Describes how to import the management packs necessary for the System Center Operations Manager CI connectors.

- How to Create a System Center Operations Manager Connector

Describes how to create a System Center Operations Manager connector and import CIs and alerts from Operations Manager 2007.

- How to Synchronize a System Center Operations Manager Connector

  Describes how to synchronize a System Center Operations Manager connector to reflect changes that you made in Operations Manager.

- How to Disable and Enable a System Center Operations Manager Connector

  Describes how to disable and enable a System Center Operations Manager connector to pause or resume data synchronization.

- How to Edit a System Center Operations Manager Connector

  Describes how to edit properties for a System Center Operations Manager connector.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Import Management Packs for System Center Operations Manager Configuration Item Connectors

For the System Center Operations Manager configuration item (CI) connector to function correctly, you have to import a set of management packs into System Center 2012 – Service Manager. The management packs and the Windows PowerShell script that you need to import the management packs are in the Service Manager installation folder. The default installation folder is \Program Files\Microsoft System Center\Service Manager 2012\Operations Manager Management Packs and System Center 2012 - Operations Manager Management Packs. Use the following procedures to import the management packs into Service Manager.

To import Operations Manager 2007 management packs for an Operations Manager CI connector

1. On the computer that is hosting the Service Manager management server, on the Windows desktop, click **Start**, point to **Programs**, point to **Windows PowerShell 1.0**, right click **Windows PowerShell**, and then click **Run as administrator**.
2. In Windows PowerShell, type the following command, and then press ENTER:

   ```
   Get-ExecutionPolicy
   ```

3. Review the output and note the current execution policy setting.
4. Type the following commands, and then press ENTER after each command:

   ```
   Set-ExecutionPolicy Unrestricted
   Set-Location \"Program Files\Microsoft System Center
   2012\Service Manager\Operations Manager Management Packs"
   ```

5. Type the following command, and then press ENTER:

   ```
   .\installOMMPs.ps1
   ```

   This command starts the Windows PowerShell script that installs the management packs. Wait for the management packs to be imported.
6. Change the execution policy back to the value that you noted in step 3. For example, type the following command to set the execution policy to Restricted, and then press ENTER:

   ```
   Set-ExecutionPolicy Restricted
   ```
7. To exit Windows PowerShell, type the following command, and then press ENTER:

   ```
   Exit
   ```

To import System Center 2012 - Operations Manager management packs for an Operations Manager CI connector

1. On the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Management Packs**.
3. In the **Tasks** pane, under **Management Packs**, click **Import**.
4. In the **Select Management Packs to Import** box, point to the drive where Service Manager is installed, and then point to Program Files\Microsoft System Center\Service Manager 2012\Operations Manager 2012 Management Packs.
5. To the right of the **File name** box, select the file type **MP files (*.mp)**.
6. In the list of files, select all of the management packs, and then click **Open**.
7. In **Import Management Packs**, select all of the management packs, and then click **Import**.
8. When the import process is complete, the message “The management pack was imported successfully” will appear.
9. Click **OK**.

How to Create a System Center Operations Manager Connector

In System Center 2012 – Service Manager, there are two types of connectors for System Center Operations Manager. You use the first type of connector, the alert connector, to automatically generate incidents that are based on Operations Manager alerts. You use the second type of connector, the configuration item (CI) connector, to import discovered objects from Operations Manager as configuration items into the Service Manager database. You can use the following procedures to create both connectors, validate them, and confirm their creation.

Note

For the Operations Manager CI connector to function correctly, you have to import a set of management packs into Service Manager. For more information, see How to Import

Management Packs for System Center Operations Manager Configuration Item Connectors.

Alerts that are generated by Operations Manager and that are sent to Service Manager do not contain user information. Therefore, when you open an incident in Service Manager, the **Affected User** box will be empty. You will not be able to save the incident form until you select an affected user. We recommend that you create a special user in Service Manager specifically for this purpose. For more information about how to create a special user, see How to Manually Create Configuration Items. This user is the user that you will assign to the **Affected User** field for all incidents created by Operations Manager.

You have the option of defining Service Manager templates that run when alerts of certain types are received. If you decide to add an alert routing rule, you can configure Service Manager to use a particular template based on alert criteria such, as priority or severity, as described in the following procedure.

There are two phases for creating the Alert connector. The first part involves creating the Alert connector on the Service Manager management server. The second part requires that you start the Operations Manager console and set up a subscription for the newly created connector. The subscription you create must be unique for the Alert connector; no connector that is created to point to Operations Manager should have a subscription that overlaps with another Operations Manager internal connector. Both phases are described in the following procedure.

To create an Operations Manager alert connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Operations Manager Alert Connector**.
4. Complete the following steps to complete the Operations Manager Alert Connector Wizard:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that the **Enable** check box is selected, and then click **Next**. Make a note of this name; you will need this name in step 7 of this procedure.
   c. On the **Server Details** page, in the **Server name** box, type the name of the server that is hosting the Operations Manager root management server. Under **Credentials**, click **New**.
   d. In the **Run As Account** dialog box, in the **Display name** box, type a name for this Run As account. In the **Account** list, select **Windows Account**.
   e. In the **User Name**, **Password**, and **Domain** fields, type the credentials for the Run As account, and then click **OK**. For more information about the permissions that are required for this Run As account, see Accounts Required During Setup in the Planning Guide for System Center 2012 - Service Manager.
   f. On the **Server Details** page, click **Test Connection**. If you receive the following

confirmation message, click **OK**, and then click **Next**:

"The connection to the server was successful."

g. On the **Alert Routing Rules** page, click **Add**.

h. In the **Add Alert Routing Rule** dialog box, create a name for the rule, select the template that you want to use to process incidents created by an alert, and then select the alert criteria that you want to use. Click **OK**, and then click **Next**.

i. On the **Schedule** page, select **Close alerts in Operations Manager when incidents are resolved or closed** or **Resolve incidents automatically when the alerts in Operations Manager are closed**, click **Next**, and then click **Create**.

5. Start the Operations Manager console.
6. Use the appropriate method, based on the version of Operations Manager 2007 you are using:
   - In Operations Manager 2007 Service Pack 1 (SP1), in the **Administration** pane, click **Product Connectors**.
   - In Operations Manager 2007 R2 and in System Center 2012 - Operations Manager, in the **Administration** pane, click **Product Connectors**, and then click **Internal Connectors**.
7. In the **Connectors** pane, click the name of the alert connector that you specified in step 4b.
8. In the **Actions** pane, click **Properties**.
9. In the **Alert Sync: <name of connector>** dialog box, click **Add**.
10. In the **Product Connector Subscription Wizard** dialog box, on the **General** page, in the **Subscription Name** box, type the name for this subscription. For example, type **All Alerts**, and then click **Next**.
11. On the **Approve groups** page, click **Next**.
12. On the **Approve targets** page, click **Next**.
13. On the **Criteria** page, click **Create**.
14. In the **Alert Sync:<name of connector>** dialog box, click **OK**.

To validate the creation of an Operations Manager alert connector

- Confirm that the connector you created is displayed in the Service Manager console in the **Connectors** pane.
- Confirm that incidents are created in Service Manager from alerts in Operations Manager.

To create an Operations Manager CI connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Operations Manager CI Connector**.

4. Complete the following steps to complete the Operations Manager CI Connector Wizard:
   a. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that the **Enable** check box is selected, and then click **Next**.
   b. On the **Server Details** page, in the **Server name** box, type the name of the server that is hosting the Operations Manager root management server.
   c. Use one of the following methods to enter credentials:
      - Under **Credentials**, select the Run As account you created for the alert connector, and then go to step 4d.
      - Under **Credentials**, click **New**. In the **User name**, **Password**, and **Domain** boxes, type the credentials for the Run As account, and then click **OK**. For more information about the permissions that are required for this Run As account, see Accounts Required During Setup in the Deployment Guide for System Center 2012 - Service Manager.
   d. On the **Server Details** page, click **Test Connection**. If you receive the following confirmation message, click **OK**, and then click **Next**:

      "The connection to the server was successful."
   e. On the **MP Selection** page, click **Select all**, or select the management packs that define the configuration items you want to import, and then click **Next**.
   f. On the **Schedule** page, click **Next**, and then click **Create**.

To validate the creation of an Operations Manager CI connector

- Confirm that the objects that Operations Manager discovered are listed as configuration items in Service Manager.

To confirm the status of an Operations Manager connector

- View the columns in the **Connector** pane; the columns contain information about the start time, the finish time, the status, and the percentage of import completion.

You can use a Windows PowerShell command to complete these tasks, as follows:

- For information about how to use Windows PowerShell to create a new Operations Manager alert connector in Service Manager, see New-SCOMAlertConnector.
- For information about how to use Windows PowerShell to create an alert rule to be used with an Operations Manager 2007 alert connector in Service Manager, see New-SCSMAlertRule.
- For information about how to use Windows PowerShell to create a new Operations Manager 2007 CI connector inService Manager, see New-SCOMConfigurationItemConnector.
- For information about how to use Windows PowerShell to retrieve connectors that are defined in Service Manager and to view their status, see Get-SCSMConnector.

How to Synchronize a System Center Operations Manager Connector

When you create a System Center Operations Manager alert connector for System Center 2012 – Service Manager, it polls Operations Manager every 30 seconds. When you create an Operations Manager configuration item (CI) connector, it synchronizes data from Operations Manager every day at the time you specified in the configured schedule. However, you can use the following procedure to manually synchronize either type of connector.

Note

The **Start Time** and **Finish Time** values are not updated when an alert connector is synchronized. These values are only updated when alert data is transferred between Operations Manager 2007 and Service Manager.

To manually synchronize an Operations Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Operations Manager connector that you want to synchronize.
4. In the **Tasks** pane, under the connector name, click **Synchronize Now**.
5. In the **Synchronize Now** dialog box, click **OK**.

To validate Operations Manager connector synchronization

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Computers**, and then click **All Windows Computers**. Verify that any new computers that were discovered in Operations Manager appear in the **All Windows Computers** pane.

How to Disable and Enable a System Center Operations Manager Connector

You can use the following procedures to disable or enable a System Center Operations Manager connector for System Center 2012 – Service Manager and validate the changes.

For example, after you configure an Operations Manager connector, if you must perform maintenance operations on the Service Manager database, you can temporarily disable the connector and suspend the data import. You can resume the data import by re-enabling the connector.

For more information about how to delete a product connector from System Center Operations Manager, see Removing an Old Product Connector on Kevin Holman's System Center blog.

To disable an Operations Manager connector

1. In the Service Manager console, click **Administration**.

2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Operations Manager connector that you want to disable.
4. In the **Tasks** pane, under the connector name, click **Disable**.
5. In the **Disable Connector** dialog box, click **OK**.

To enable an Operations Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Operations Manager connector that you want to enable.
4. In the **Tasks** pane, under the connector name, click **Enable**.
5. In the **Enable Connector** dialog box, click **OK**.

To validate the status change of an Operations Manager connector

1. Wait 30 seconds. Then, in the Service Manager console, click **Administration**, and then click **Connectors**.
2. In the **Connectors** pane, locate the connector for which you have changed the status, and verify the value in the **Enabled** column.

You can use Windows PowerShell commands to complete these tasks and other related tasks, as follows:

- For information about how to use Windows PowerShell to start a Service Manager connector, see Start-SCSMConnector.
- For information about how to use Windows PowerShell to retrieve connectors that are defined in Service Manager and view their status, see Get-SCSMConnector.
- For information about how to use Windows PowerShell to update the properties of a Service Manager connector, see Update-SCSMConnector.

How to Edit a System Center Operations Manager Connector

After you install a System Center Operations Manager alert connector and configuration item (CI) connector, you can edit the connectors. For example, you can use the following procedure to add more management packs to the CI connector.

To edit an Operations Manager CI connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Operations Manager connector that you want to edit.
4. In the **Tasks** pane, under the connector name, click **Properties**.

5. In the **Edit** dialog box, in the left pane, click **Management Packs**.
6. In the **Management Packs** pane, click **Refresh**.
7. In the **Credentials** dialog box, enter the credentials to connect to Operations Manager, and then click **OK**.
8. In the **Management Packs** list, select the management packs that define the configuration items that you want to import, and then click **OK**.

Importing Data from System Center Configuration Manager

This section describes how to create, configure, disable, and enable a Configuration Manager connector, and how to customize the Configuration Manager extended SMS_def.mof file for collecting hardware information. You use the connector to import data from System Center Configuration Manager into System Center 2012 – Service Manager.

You have an option to create a connector for either System Center Configuration Manager 2007 or System Center 2012 - Configuration Manager. The connector for System Center 2012 - Configuration Manager recognizes User-device Affinity and Mobile Devices and synchronizes them in the Service Manager database.

Importing Data from Configuration Manager Topics

- About Importing Data from System Center Configuration Manager

  Provides an overview of how to import data from Configuration Manager by using a connector.
- How to Create a Configuration Manager Connector

  Describes how to create a Configuration Manager connector and import data from Configuration Manager.
- How to Disable and Enable a Configuration Manager Connector

  Describes how to disable and enable a Configuration Manager connector to pause and resume data import from Configuration Manager.
- How to Synchronize a Configuration Manager Connector

  Describes how to synchronize the data in Configuration Manager with the Service Manager database.
- How to Configure a Configuration Manager Connector for an Extended SMS_def.mof File

  Describes how to customize the default Configuration Manager 2007 SMS_def.mof file to extend the hardware information that is collected.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager

- Operations Guide for System Center 2012 – Service Manager

About Importing Data from System Center Configuration Manager

You can import data from the System Center Configuration Manager site database into the System Center 2012 – Service Manager database. This automatically creates and populates configuration items for the hardware and software that you want to manage in Service Manager. After you import data from System Center Configuration Manager, you can attach the respective configuration items to relevant incidents, and the information in the configuration items will be available to analysts working on the incident.

Note

Service Manager imports data from Microsoft System Center Configuration Manager 2007 with Service Pack 1 (SP1), Microsoft System Center Configuration Manager 2007 R2, or System Center 2012 - Configuration Manager.

By using a Configuration Manager connector, you can import configuration baselines from System Center Configuration Manager and then use these configuration baselines to automatically generate incidents for noncompliant configuration items. For more information about this option, see **How to Configure Desired Configuration Management to Generate Incidents**.

For information about Microsoft Operations Framework (MOF) implementation of change and configuration, see Position of the Change and Configuration SMF Within the MOF IT Service Lifecycle.

Complete the Data Warehouse Registration Process

Before you create the Configuration Manager connector, you must make sure that the Data Warehouse Registration process is complete. For more information, see **How to Determine When Data Warehouse Registration Is Complete** in the Deployment Guide for System Center 2012 - Service Manager.

Additional Data in System Center 2012 - Configuration Manager

Additional data in System Center 2012 - Configuration Manager includes User-Device Affinity (UDA), Mobile Device Data, and Software Request Data. UDA data from System Center 2012 - Configuration Manager more accurately determines who the primary user of a computer or device is. The UDA data collected by the Service Manager System Center 2012 - Configuration Manager connector is used to populate the UsesComputer and PrimaryUser information in the Service Manager database.

Mobile device data for Windows Phones, Windows Mobile Phones, and Nokia devices will be collected by the Service Manager Configuration Manager connector. Data from other mobile devices such as iPhone, BlackBerry, and Android-based phones will be collected when you are using the Configuration Manager Exchange Server connector. For more information about the Exchange connector, see What's New in Configuration Manager 2012. Mobile device data will be imported into the Service Manager database as configuration items, and it can be associated with work items, incident management, and change management.

Software request data will be used in support of self-service software request integration with System Center 2012 - Configuration Manager. The administrative category data from Configuration Manager will be used to select which Service Request templates to apply when creating a request from the Self-Service Portal.

Schedule

You can configure the Configuration Manager connector to update the Service Manager database on a recurring schedule. You can also temporarily suspend the importation of data from Configuration Manager by disabling the connector. For example, you can disable the connector when maintenance is performed on the Configuration Manager site database because you know that the maintenance process temporarily creates inaccurate data. When appropriate, you can re-enable the connector and resume importing data.

Extended Hardware Inventory with Configuration Manager 2007

In System Center Configuration Manager 2007, you can extend the hardware inventory by collecting an inventory of additional Windows Management Instrumentation (WMI) classes, additional WMI class attributes, registry keys, and other customizations to accommodate your organization's requirements. For more information about extending the hardware inventory in Configuration Manager 2007, see How to Extend Hardware Inventory.

If you have extended the hardware inventory in Configuration Manager 2007, you must create a new Configuration Manager 2007 Connector management pack in Service Manager to collect the extended hardware inventory. This new management pack can contain only the information required to collect the extended hardware inventory from Configuration Manager 2007, or it can consist of everything from the original Configuration Manager 2007 Connector management pack plus the new extended hardware inventory. For information about creating a new connector management pack, see **Configure a Configuration Manager Connector for an Extended SMS_DEF.MOF File**.

Importing Software Configuration Items

You can import software configuration items with the Configuration Manager Connector by importing the following asset intelligence reporting classes in System Center Configuration Manager. These classes should be enabled in Configuration Manager before you configure the Configuration Manager connector in Service Manager. For more information about enabling Asset Intelligence in Configuration Manager, see How to Enable Asset Intelligence.

- SMS_InstalledSoftware
- SMS_SystemConsoleUsage
- SMS_SystemConsoleUser
- SoftwareLicensingService
- SoftwareLicensingProduct

If software for a particular computer does not appear in the **All Software** view in the Configuration Items workspace, you should review the Operations Manager event log on the

Service Manager primary management server. You should look for events with sources of OpsMgr Connector and Lfx Service to determine if there are any errors.

See Also

How to Configure a Configuration Manager Connector for an Extended SMS_def.mof File

How to Create a Configuration Manager Connector

How to Disable and Enable a Configuration Manager Connector

Appendix C - Mapping System Center 2012 - Service Manager Properties to Configuration Manager Database Views

How to Create a Configuration Manager Connector

You can use the following procedures to create a connector to import data from Microsoft System Center Configuration Manager 2007 with Service Pack 1 (SP1) or System Center 2012 - Configuration Manager into System Center 2012 – Service Manager and confirm the status of the connector.

Important

Before you can create the Configuration Manager connector, you have to verify that System Center Configuration Manager is installed in your environment, and you have to turn on Windows User Account Control (UAC). For more information about UAC, see User Account Control.

To create a Configuration Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Configuration Manager Connector**. The System Center Configuration Manager Connector Wizard starts.
4. On the **Before You Begin** page, click **Next**.
5. On the **General** page, do the following:
   a. In the **Name** box, type a name for the new connector. For example, type **Configuration Manager Connector to Seattle**.
   b. In the **Description** box, type a description for the new connector. For example, type **A Configuration Manager connector to site Seattle**.
   c. Make sure that the **Enabled** check box is selected, and then click **Next**.
6. On the **Select Management Pack** page, in the **Management Pack** list, select either **System Center Configuration Manager Connector Configuration** or **System Center Configuration Manager 2012 Connector Configuration**, and then click **Next**.
7. On the **Connect to System Center Configuration Manager Database** page, do the following:
   a. In the **Database Server Name** box, type the server name of the server that is hosting

the System Center Configuration Manager site database and the database named instance, if applicable. For example, at the hypothetical Woodgrove Bank, you might type **woodgrove\instance1** if the System Center Configuration Manager database is on a named instance of Microsoft SQL Server, or type **woodgrove** if the database is on a default instance of SQL Server.

b. In the **Database Name** box, type the name of the System Center Configuration Manager site database. For example, type **SMS_CM1**.

c. In the **Credentials** area, select a Run As account, or create a new Run As account. The user account that you specify as the Run As account must be a member of the smsdbrole_extract and the db_datareader groups for the Configuration Manager site database.

d. In the **Credentials** area, click **Test Connection**.

e. In the **Credentials** dialog box, in the **Password** box, type the password for the account, and then click **OK**.

f. In the **Test Connection** dialog box, if you receive the following confirmation message, click **OK**:

   The connection to the server was successful.

g. Click **Next**.

8. On the **Collections** page, select the appropriate collection, and then click **Next**.
9. On the **Schedule** page, in the **Synchronize** list, set the frequency and time of synchronization, and then click **Next**.
10. On the **Summary** page, confirm the connector settings you made, and then click **Create**.
11. On the **Confirmation** page, make sure that you receive the following confirmation message:

    "You have successfully completed the System Center Configuration Manager Connector Wizard."

    Then, click **Close**.

    Note

    The System Center Configuration Manager Connector Wizard may take several hours to import data from System Center Configuration Manager.

To validate the creation of a Configuration Manager connector

1. Confirm that the Configuration Manager connector that you created is displayed in the **Connectors** pane.
2. In the Service Manager console, click **Configuration Items**. In the **Configuration Items** pane, expand **Configuration Items**, expand **Computers**, and then click **All Windows Computers**. Verify that the intended computers from Configuration Manager 2007 appear in the **All Windows Computers** pane.
3. In the middle pane, double-click a newly imported computer. Verify that the appropriate computer details appear in the computer form.

To confirm the status of a Configuration Manager connector

- View the columns in the **Connector** pane; the columns contain information about the start time, the finish time, the status, and the percentage of completion.

You can use a Windows PowerShell command to create a new Configuration Manager 2007 connector. For information about how to use Windows PowerShell to create a new Configuration Manager 2007 connector in Service Manager, see New-SCCMConnector.

How to Disable and Enable a Configuration Manager Connector

You can use the following procedures to disable or enable a System Center Configuration Manager connector and validate the status of the change.

To disable a Configuration Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Configuration Manager connector that you want to disable. For example, click **Configuration Manager connector to SEA**.
4. In the **Tasks** pane, under the connector name, click **Disable**.

   Note
   If you disable a connector while it is synchronizing data, the synchronization process may not stop. However, a disabled connector will not import any new data from a Configuration Manager database from that point forward.

To enable a Configuration Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Configuration Manager connector that you want to enable. For example, click **Configuration Manager connector to SEA**.
4. In the **Tasks** pane, under the connector name, click **Enable**.

To validate the status change of a Configuration Manager connector

1. After you disable or enable the connector, wait 30 seconds. Then, in the Service Manager console, click **Administration**, and then click **Connectors**.
2. In the **Connectors** pane, locate the connector for which you have changed status, and verify the value in the **Enabled** column.
3. If you enabled the connector, verify that the connector resumes synchronization according to the schedule. If you disabled the connector, verify that the connector no longer synchronizes according to the schedule.

You can use Windows PowerShell commands to complete these tasks and other related tasks, as follows:

- For information about how to use Windows PowerShell to start a Service Manager connector, see Start-SCSMConnector.
- For information about how to use Windows PowerShell to retrieve connectors that are defined in Service Manager and view their status, see Get-SCSMConnector.
- For information about how to use Windows PowerShell to update the properties of a Service Manager connector, see Update-SCSMConnector.

How to Synchronize a Configuration Manager Connector

To ensure that the System Center 2012 – Service Manager database is up to date, the System Center Configuration Manager 2007 connector synchronizes with Configuration Manager every day after the initial synchronization. However, you can use the following procedures to synchronize the connector manually and validate that the connector synchronized.

To manually synchronize a Configuration Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Configuration Manager connector that you want to synchronize.
4. In the **Tasks** pane, under the name of the connector, click **Synchronize Now**.

   Note
   Depending on the amount of data that is imported, you might have to wait for the import to be completed.

To validate that a Configuration Manager connector synchronized

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Computers**, and then click **All Windows Computers**. Verify that any new computers in Configuration Manager 2007 appear in the middle pane.

How to Configure a Configuration Manager Connector for an Extended SMS_def.mof File

Microsoft System Center Configuration Manager 2007 hardware inventory collects and then provides system information, such as available disk space, processor type, and operating system, about each computer in the Configuration Manager 2007 hierarchy. In Configuration Manager

2007, users can customize the default Configuration Manager 2007 SMS_def.mof file to extend the hardware inventory information that is collected.

When you create a Configuration Manager connector in Service Manager, you can select the default System Center Configuration Manager Connector Configuration management pack that must be used for that connector. By using the default management pack, the connector imports hardware, software, and desired configuration management information for the computers that are in the system.

If the Configuration Manager 2007 SMS_def.mof file has been extended to collect additional hardware inventory data, which you also want to import into Service Manager, you must create a new custom management pack that defines that additional data. Then, you have to create a new Configuration Manager connector and configure it to use the new custom management pack.

Importing Extended Hardware Inventory Data from Configuration Manager

To import extended hardware inventory data from Configuration Manager 2007, you must author a custom Configuration Manager 2007 connector management pack. There are two approaches to implementing a custom Configuration Manager connector:

- Create a custom Configuration Manager connector management pack that defines the extended data that you want to import and then create two connectors. Configure one connector to use the default System Center Configuration Manager Connector Configuration management pack to import the data that is defined by default. Configure the second connector to use the custom management pack to import the additional extended data.
- Customize the default System Center Configuration Manager Connector Configuration management pack to also include the additional extended data. Create a single connector that is configured to use the custom management pack to import all the information that you must have.

This topic provides the information that you must have to implement the first approach that is described earlier. It provides the details that you must have so that you can develop a custom Configuration Manager connector management pack that imports the extended hardware inventory from Configuration Manager 2007.

The high-level steps to importing extended hardware inventory data are as follows:

1. Create a custom Configuration Manager Connector Configuration management pack with the definitions for the extended data.
2. Import the custom management pack into Service Manager. After you import the management pack, Service Manager processes the directives in the management pack to create staging tables and to run any install Structured Query Language (SQL) scripts, as defined in the management pack.
3. Create a Configuration Manager connector and configure it to use the custom management pack.
4. The Configuration Manager connector imports the data.

Working with a Custom Configurations Manager Connector Management Pack

Consider the following tips when you are working with a custom Configurations Manager Connector management pack:

- Semantic errors in the connector configuration templates in the management pack do not prevent the management pack from being imported, and they are logged to the event log. In this case, you must delete the management pack, correct the errors, and reimport the management pack.
- After creating a Configuration Manager connector, you cannot modify its management pack selection. Instead, you must delete that connector and then create a new one with the desired management pack selection.
- To ensure a successful deletion of a management pack, you must delete any connectors that are configured to use the management pack that you want to delete and then delete the management pack.

  When you delete a custom Configurations Manager Connector management pack, Service Manager tries to delete all related staging tables that were created during the management pack import. Then, Service Manager runs any scripts that are defined in the **Uninstall** section of the management pack.
- Unlike other management packs, the custom Configuration Manager 2007 Connector management pack cannot be versioned. Importing a later version of the management pack will succeed. However, the connector configuration in the management pack will be ignored, or it might cause validation errors that are logged to the event log.

Creating a Custom Configuration Manager Connector Configuration Management Pack

A custom Configuration Manager Connector Configuration management pack is similar in structure to the default Configuration Manager Connector management pack. It must contain the two object templates **DataProvider** and **DataConsumer** that specify how the data should be imported and applied.

DataProvider Section

The **DataProvider** section provides information, such as which data to import, that you must have when you are importing data from Configuration Manager 2007 into the staging tables of **LinkingFramework**. The **DataProvider** section includes the queries that run on the Configuration Manager 2007 site database; directives for staging table creation; custom SQL scripts; and information that is relevant for incremental synchronization, such as watermarking and batching.

DataConsumer Section

The **DataConsumer** section provides information about reading the data from staging tables and writing it to the **ServiceManager** database's instances space, such as **Entities** or **Relationships**. The **DataConsumer** section includes queries that run on the staging tables; mapping to the Service Manager type system; custom SQL scripts; and information that is relevant for incremental synchronization, such as watermarking and batching.

Structure of the DataProvider and DataConsumer Object Templates Sections

Basically, the **DataProvider** and the **DataConsumer** are object templates that are targeted to a projection type. The following code shows the general structure of the **DataProvider** and the **DataConsumer** sections:

```
<TypeProjection ID="System.LinkingFramework.DataConnector.Projection"
Accessibility="Public" Type="System.LinkingFramework.DataConnector">
          <Component Alias="DataTable"
Path="$Context/Path[Relationship='System.LinkingFramework.ConnectorEmbedsTables'
TypeConstraint='System.LinkingFramework.DataTable']$">
            <Component Alias="Field"
Path="$Context/Path[Relationship='System.LinkingFramework.TableEmbedsFields']$" />
          </Component>
          <Component Alias="DataCollection"
Path="$Context/Path[Relationship='System.LinkingFramework.ConnectorEmbedsCollections'
TypeConstraint='System.LinkingFramework.DataCollection']$" />
 </TypeProjection>
```

In this code, **DataTable**, **Field**, and **DataCollection** are defined as follows:

- **DataTable**. The smallest data unit that is defined for data transfer. It is a declaration of what data to retrieve from the external data source. It also defines dependencies between different data tables and when data batching, watermarking, and grooming have finished.
- **Field**. A single column in a data table.
- **DataCollection**. A set of data tables to be transferred in one data transfer job or session. It defines which data tables are included in this data collection.

Properties in the Custom Management Pack

The following table provides the details about each property in the custom Configuration Manager Connector Configuration management pack. Use these guidelines when you create the custom management pack.

Property	Expected value	Validation after import
ID	For both **DataProvider** and **DataConsumer** templates—as indicated in the sample	Yes
DataConnector Properties		
DataConnectorName	For both **DataProvider** and **DataConsumer** templates—identical	Yes

Property	Expected value	Validation after import
	to the values in the sample	
IsProvider	In **DataProvider** template—True In **DataConsumer** template—False	Yes
SolutionName	A comment. For example, it can indicate the type of the imported data.	An attempt to import a management pack in which the solution name is already being used; it causes an error that is logged to the event log.
Entrypoint, EntryAssembly & WinformUIAssembly	Identical to the value in the sample	
InstallSQLScripts section	SQL scripts that must run after the staging tables are set up. They are usually used in the **DataConsumer** template to configure views that display data from the staging tables. Everything that is enclosed between the <Script></Script> tags is expected to be valid SQL script. Therefore, for comments, you must use the '/*' and the '*/' multi-line comment delimiters instead of the standard XML comment tags.	Not validated. Use custom table names to ensure that this does not cause overwriting or changing any tables except the ones that are declared in the management pack.
UnInstallSQLScripts section	SQL scripts that must run after you delete the Configuration Manager Connector	Not validated. Use custom table names to ensure that this does not cause overwriting or changing any tables except the tables that are declared in the management pack.

Property	Expected value	Validation after import
	management pack in the Service Manager console. Everything that is enclosed between the <Script></Script> tags is expected to be valid SQL script. Therefore, for comments, you must use the '/*' and the '*/' multi-line comment delimiters instead of the standard XML comment tags.	
DisableParallelProcessing	True	
DataTable Properties		
DataName	The table from which to import data. It is used in the user interface (UI) and not used in queries.	
StageTableName	The name of the staging table. It must be unique.	An attempt to import a management pack, in which the table name is already being used, causes an error to be logged to the event log.
WatermarkField	The name of the **rowversion** column	
WatermarkType	Possible values are: • 0—Indicates **DateTime** type • 1—Indicates the **Timestamp** type • (-1)—Indicates no watermarking, in which case **WatermarkField** becomes optional	Other types of watermarking are not supported.

Property	Expected value	Validation after import
BatchIdField	The name of the column that has good selectivity; used to separate incremental data into batches when importing to staging tables	
BatchIdType	Possible values are: • 0—Int • (-1)—No batching, in which case **BatchIdField** becomes optional	Integer column
BatchIdSize	The size of the batch, if batching is used. A high number indicates that much data is being read or written at the same time. The recommended value is 500.	Integer column
UseCache	True	
GroomType	Possible values are: • 1—The data in staging tables can be groomed after it is transferred to the Service Manager database. • 2—The data in staging tables is groomed only after it is marked as deleted in the Configuration Manager database and	

Property	Expected value	Validation after import
	has also been deleted in the Service Manager database because of the Service Manager connector synchronization.	

QueryString	The actual query that Configuration Manager 2007 uses to retrieve the requested data. The query must be of the form:
	`SELECT …`
	`FROM …`
	`WHERE …`
	`ORDER BY …`
	The WHERE clause can contain the "$COLLECTIONLIST" token. During synchronization, this token is replaced by the collections that are specified in the System Center Configuration Manager Connector Wizard.
	The data that is exposed by Configuration Manager 2007 SCCM_Ext.* views is supported for import. This data can be extended by using standard
		Not validated. All queries have an Lfx_Status column with value "U" or "D," indicating whether the row represents an Update or a Delete operation.

Property	Expected value	Validation after import
	sms_def.mof extensions or by using noidmifs. Other tables are not supported. Notably, subqueries are not supported, but joins to other tables are supported.	
CollectionName	A name for a group of data tables; this name must be unique. Tables in the same collection cannot depend on each other.	An attempt to import a management pack, in which the collection name is already being used, causes an error to be logged to the event log.
PrimaryKeyName	A section that declares the unique primary key name for the staging table.	An attempt to import a management pack, in which the key name is already being used, causes an error to be logged to the event log.
DependOnDataTable	The name or names of **DataTable** that must be synchronized first before this one. Typically, this is used to synchronize the staging table before the system reads it in the Consumer view. If you are using multiple collections, dependency should be expressed only between tables in different collections.	Not validated
DataField Properties		
Name, Type, AllowNull	These are required fields for any column	Not validated

Property	Expected value	Validation after import
	type. Supported types are **int**, **nvarchar**, **datetime** and **xml**.	
PrimaryKeyACs, PrimaryKeyPosition	If part of primary key, indicates the position from the left in the primary key. Lfx adds two internal use columns (Lfx_Status, Lfx_SourceId) to the PK at the end.	
Collation	DATABASE_DEFAULT	Not validated
DataCollection Properties		
DataCollectionName	Must be identical to what is referenced by a **DataTable** property	An attempt to import a management pack, in which the collection name is already being used, causes an error to be logged to the event log.
StagingName	In DataProvider template—DefaultCache In DataConsumer template—Not present	Not validated
DataTables	Comma-separated value (CSV) list of tables referencing this collection	

Settings	In **DataProvider** template—Not present
	In **DataConsumer** template—Indicates type mapping
		Escaped XML with following syntax:
		`<TypeName>Microsoft.Windows.Computer</TypeName>`
		`<MPName>Microsoft.Windows.Library</MPName>`
		`<MPVersion>version of MP</MPVersion>`
		`<MPToken>token for MP</MPToken>`

Sample of Custom Configuration Manager Connector Configuration Management Packs

The following are schema definitions and Configuration Manager Connector management pack samples that import data from the Configuration Manager 2007 SCCM_Ext.vex_GS_PC_BIOS view.

Refer to the table earlier in this topic for more information about the properties of these management packs. Use an XML editor, such as the editor in Microsoft Visual Studio, to modify these samples to fit your import scenarios.

Importing Data from a Hosted Class

When you are specifying a class that is hosted, the view in the **DataConsumer** template should include columns for the key property of the parent class. In this sample, the class that contains the BIOS information is hosted under a computer.

In this example, the Configuration Manager Connector Configuration management pack has two collections in the **DataProvider** and in the **DataConsumer** sections, one for importing the computers data and the second to import the BIOS data.

Class Definition

```
<ManagementPack xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" ContentReadable="true"
SchemaVersion="1.1" OriginalSchemaVersion="1.1">
  <Manifest>
    <Identity>
      <ID>SampleBIOSMP</ID>
      <Version>1.0.0.0</Version>
    </Identity>
    <Name>BIOS Class MP</Name>
    <References>
      <Reference Alias="System">
        <ID>System.Library</ID>
        <Version>7.0.5229.0</Version>
        <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
      </Reference>
      <Reference Alias="Windows">
        <ID>Microsoft.Windows.Library</ID>
        <Version>7.0.5229.0</Version>
        <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
      </Reference>
```

```
    </References>
  </Manifest>
  <TypeDefinitions>
    <EntityTypes>
      <ClassTypes>
        <ClassType ID="HostedCustomClass" Accessibility="Public"
Base="System!System.ConfigItem" Hosted="true" Abstract="false">
            <Property ID="SerialNumber" Type="string" Key="true"/>
        </ClassType>
      </ClassTypes>
      <RelationshipTypes>
        <RelationshipType ID="Microsoft.Windows.ComputerHostsBIOS" Accessibility="Public"
Base="System!System.Hosting">
          <Source ID="Computer" Type="Windows!Microsoft.Windows.Computer" />
          <Target ID="BIOSClass" Type="HostedCustomClass" />
        </RelationshipType>
      </RelationshipTypes>
    </EntityTypes>
  </TypeDefinitions>
</ManagementPack>
```

Configuration Manager Connector Configuration management pack

```
<ManagementPack xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform" ContentReadable="true"
SchemaVersion="1.1" OriginalSchemaVersion="1.1">
  <Manifest>
    <Identity>
      <ID>CnfgMgrBiosSample</ID>
      <Version>7.0.5229.0</Version>
    </Identity>
    <Name>CnfgMgrBiosSample</Name>
    <References>
      <Reference Alias="System">
        <ID>System.Library</ID>
        <Version>7.0.5229.0</Version>
```

```
        <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
      </Reference>
      <Reference Alias="LFX">
        <ID>ServiceManager.LinkingFramework.Library</ID>
        <Version>7.0.5229.0</Version>
        <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
      </Reference>
    </References>
  </Manifest>
  <Templates>
    <ObjectTemplate
ID="DataProvider.Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms"
TypeID="LFX!System.LinkingFramework.DataConnector.Projection">
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/DataConnectorNa
me$">
          Microsoft_EnterpriseManagement_ServiceManager_Connector_Sms
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/IsProvider$">
          True
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/SolutionName$">
SampleBIOS</Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/EntryPoint$">
          Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms.SmsConnector
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/EntryAssembly$"
>
          Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms,
          Version="7.0.5000.0",
          Culture=neutral,
```

```
          PublicKeyToken="31bf3856ad364e35"
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/WinFormUIAssemb
ly$">
          Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms.SmsConnector,
          Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms,
Version="7.0.5000.0", Culture=neutral,
          PublicKeyToken="31bf3856ad364e35"
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/InstallSQLScrip
ts$"></Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/DisableParallel
Process$">
          True
      </Property>

      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsTables'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataTable']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DataName$">SCCM_Ext
.Sample_vex_R_System</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/StageTableName$">Sa
mple_SMS_vex_R_System</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkField$">S.
[rowversion]</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkType$">1</
Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdField$">S.[R
esourceID]</Property>
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">2000<
/Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">true</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/GroomType$">2</Prop
erty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CD
ATA[
                            SELECT S.ResourceID,
                                S.ChangeAction as Lfx_Status,
                                S.Netbios_Name0,
                                S.Resource_Domain_OR_Workgr0
                            FROM SCCM_Ext.vex_R_System S
                            INNER JOIN SCCM_Ext.vex_FullCollectionMembership CM
                                ON S.ResourceID = CM.ResourceID
                            INNER JOIN SCCM_Ext.vex_Collection C
                                ON C.CollectionID = CM.CollectionID
                            WHERE ((S.ChangeAction = 'U' AND S.Client_Type0 != 3 AND
S.Hardware_ID0 IS NOT NULL)
                                  OR S.ChangeAction = 'D')
                                  AND $COLLECTIONLIST
                            ORDER BY S.rowversion
                   ]]>
</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">BI
OSComputers</Property>
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/PrimaryKeyName$">[S
ample_SMS_PK_v_R_SYSTEM]</Property>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">[ResourceID]</Pr
operty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Prop
erty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">0<
/Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</P
roperty>
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">Netbios_Name0</P
roperty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Proper
ty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">64</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE_DE
FAULT</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Prope
rty>
```

```
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">Resource_Domain_
OR_Workgr0</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Proper
ty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">255</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE_DE
FAULT</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Prope
rty>
        </Object>
      </Object>

      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsTables'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataTable']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DataName$">SCCM_Ext
.Sample_vex_GS_COMPUTER_SYSTEM</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/StageTableName$">Sa
mple_SMS_vex_GS_COMPUTER_SYSTEM</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkField$">CS
.[rowversion]</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkType$">1</
Property>
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdField$">CS.[
ResourceID]</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">2000<
/Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">true</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/GroomType$">2</Prop
erty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CD
ATA[
                            SELECT CS.ResourceID,
                                    CS.GroupKey,
                                    CS.ChangeAction as Lfx_Status,
                                    CS.Name0,
                                    CS.Domain0
                            FROM SCCM_Ext.vex_GS_COMPUTER_SYSTEM CS
                            INNER JOIN SCCM_Ext.vex_FullCollectionMembership CM
                                ON CS.ResourceID = CM.ResourceID
                            INNER JOIN SCCM_Ext.vex_Collection C
                                ON C.CollectionID = CM.CollectionID
                            WHERE $COLLECTIONLIST
                            ORDER BY CS.rowversion
                    ]]>
</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">BI
OSComputers</Property>
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/PrimaryKeyName$">[S
ample_SMS_PK_v_GS_COMPUTER_SYSTEM]</Property>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">[ResourceID]</Pr
operty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Prop
erty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">0<
/Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</P
roperty>
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">[GroupKey]</Prop
erty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Prop
erty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">1<
/Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</P
roperty>
```

```
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">[Name0]</Propert
y>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Proper
ty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">64</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE_DE
FAULT</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Prope
rty>
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">[Domain0]</Prope
rty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Proper
ty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">32</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE_DE
FAULT</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Prope
rty>
        </Object>
```

```
      </Object>

      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsTables'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataTable']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DataName$">SCCM_Ext
.vex_GS_PC_BIOS</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/StageTableName$">Sa
mple_SMS_vex_GS_PC_BIOS</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkField$">S.
[rowversion]</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkType$">1</
Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdField$">S.[R
esourceID]</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">2000<
/Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">true</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/GroomType$">2</Prop
erty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CD
ATA[
                      SELECT S.ChangeAction as Lfx_Status,
                      S.ResourceID,
```

```
                    S.BatchingKey,
                    S.GroupKey,
                    S.SerialNumber0
                    FROM SCCM_Ext.vex_GS_PC_BIOS S
                    INNER JOIN SCCM_Ext.vex_FullCollectionMembership CM
                      ON S.ResourceID = CM.ResourceID
                    INNER JOIN SCCM_Ext.vex_Collection C
                      ON C.CollectionID = CM.CollectionID
                    WHERE C.ChangeAction = 'U' AND CM.ChangeAction = 'U' AND
$COLLECTIONLIST
                    ORDER BY S.rowversion
                  ]]>
        </Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">Sa
mple_SMS_PROVIDER_BIOS_COLLECTION</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/PrimaryKeyName$">[S
ample_SMS_PK_v_GS_BIOS1]</Property>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">[ResourceID]</Pr
operty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Prop
erty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">0<
/Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</P
roperty>
```

```
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">BatchingKey</Pro
perty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Prop
erty>
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">GroupKey</Proper
ty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Prope
rty>
        </Object>
        <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.TableEmbedsFields'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.Field']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Name$">SerialNumber0</P
roperty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Proper
ty>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">34</Property>
```

```
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE_DE
FAULT</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Prope
rty>
        </Object>
      </Object>

      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsCollections'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataCollection']$">
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollection
Name$">BIOSComputers</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/StagingName$">
DefaultCache</Property>
          <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">S
CCM_Ext.Sample_vex_R_System,SCCM_Ext.Sample_vex_GS_COMPUTER_SYSTEM</Property>
      </Object>
      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsCollections'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataCollection']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollection
Name$">Sample_SMS_PROVIDER_BIOS_COLLECTION</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/StagingName$">
DefaultCache</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">S
CCM_Ext.vex_GS_PC_BIOS</Property>
      </Object>
    </ObjectTemplate>
```

```
    <ObjectTemplate
ID="DataConsumer.Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms"
TypeID="LFX!System.LinkingFramework.DataConnector.Projection">
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/DataConnectorNa
me$">
          MomStore
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/IsProvider$">
          False
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/SolutionName$">
SampleBIOS</Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/EntryPoint$">

Microsoft.EnterpriseManagement.ServiceManager.Linking.Consumer.OperationalStore.Operation
alStoreConsumer
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/EntryAssembly$"
>
  Microsoft.EnterpriseManagement.ServiceManager.Linking.Consumer.OperationalStore,
  Version="7.0.5000.0",
  Culture=neutral,
  PublicKeyToken="31bf3856ad364e35"
      </Property>
      <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/InstallSQLScrip
ts$"><![CDATA[
                        <Script>
                             if not object_id('[LFXSTG].[v_Sample_SMS_BIOSComputer]') is
null
                                drop view [LFXSTG].[v_Sample_SMS_BIOSComputer];
```

```
                            exec ('
                               CREATE VIEW [LFXSTG].[v_Sample_SMS_BIOSComputer] AS
                                   SELECT S.Lfx_RowId,
                                          S.Lfx_SourceID,
                                          S.Lfx_Timestamp,
                                          S.Lfx_Status,
                                          CS.Name0 AS ''DisplayName'',
                                          COALESCE(CS.Name0, S.Netbios_Name0)
                                   + ''.'' + COALESCE(CS.Domain0,
S.Resource_Domain_OR_Workgr0) AS ''PrincipalName''
                                   FROM LFXSTG.Sample_SMS_vex_R_System S
                                   INNER JOIN LFXSTG.Sample_SMS_vex_GS_COMPUTER_SYSTEM
CS
                                        ON S.ResourceID = CS.ResourceID AND
S.Lfx_SourceId = CS.Lfx_SourceId
                                   WHERE S.Netbios_Name0 IS NOT NULL
                                       AND S.Resource_Domain_OR_Workgr0 IS NOT NULL
                               ');
                        </Script>


                        <Script>
                            if not object_id('[LFXSTG].[v_Sample_BIOS]') is null
                               drop view [LFXSTG].[v_Sample_BIOS]
                            exec ('
                               CREATE VIEW [LFXSTG].[v_Sample_BIOS] AS
                                   SELECT P.Lfx_RowId AS Lfx_RowId,
                                       P.Lfx_SourceId,
                                       P.Lfx_Timestamp AS Lfx_Timestamp,
                                       P.Lfx_Status as Lfx_Status,
                                       P.SerialNumber0 AS ''SerialNumber'',
                                       COALESCE(CS.Name0, S.Netbios_Name0) + ''.'' +
COALESCE(CS.Domain0, S.Resource_Domain_OR_Workgr0) AS ''PrincipalName''
                                   FROM [LFXSTG].Sample_SMS_vex_GS_PC_BIOS P
                                   INNER JOIN [LFXSTG]. Sample_SMS_vex_R_System S
```

```
                                        ON P.ResourceID=S.ResourceID AND P.Lfx_SourceId =
S.Lfx_SourceId
                                    INNER JOIN [LFXSTG].
Sample_SMS_vex_GS_COMPUTER_SYSTEM CS
                                        ON S.ResourceID=CS.ResourceID
                                           AND S.Lfx_SourceId = CS.Lfx_SourceId
                                ')
                        </Script>
                    ]]>
        </Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/UninstallSQLScr
ipts$"><![CDATA[
                        <Script>
                             if not object_id('[LFXSTG].[v_Sample_SMS_BIOSComputer]') is
null
                                 drop view [LFXSTG].[v_Sample_SMS_BIOSComputer];
               </Script>


                        <Script>
                             if not object_id('[LFXSTG].[v_Sample_BIOS]') IS NULL
                                 drop view [LFXSTG].[v_Sample_BIOS];
               </Script>
                    ]]>
        </Property>


      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsTables'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataTable']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DataName$">Sample_S
MS_Computer</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkField$">E.
Lfx_Timestamp</Property>
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkType$">0</
Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdField$">E.Lf
x_RowId</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">500</
Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">false</P
roperty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CD
ATA[
                            SELECT * FROM [LFXSTG].v_Sample_SMS_BIOSComputer E
                    ]]>
        </Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">Sa
mple_SMS_Computers_COLLECTION</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DependOnDataTable$"
>SCCM_Ext.Sample_vex_GS_COMPUTER_SYSTEM,SCCM_Ext.Sample_vex_R_System</Property>
      </Object>


      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsTables'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataTable']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DataName$">Sample_S
MS_BIOS_CONSUMER_VIEW</Property>
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkField$">C.
Lfx_Timestamp</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/WatermarkType$">0</
Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdField$">C.Lf
x_RowId</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Pr
operty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">500</
Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">False</P
roperty>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CD
ATA[
                        select C.* from [LFXSTG].v_Sample_BIOS C
                    ]]>
        </Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">Sa
mple_SMS_BIOS_CONSUMER_COLLECTION</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/DependOnDataTable$"
>SCCM_Ext.vex_GS_PC_BIOS, Sample_SMS_Computer</Property>
      </Object>

      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsCollections'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataCollection']$">
```

```
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollection
Name$">Sample_SMS_Computers_COLLECTION</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">S
ample_SMS_Computer</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/Settings$"><![
CDATA[
<TypeName
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">Microsoft.Windows.Co
mputer</TypeName>
<MPName
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">Microsoft.Windows.Li
brary</MPName>
<MPVersion
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">7.0.5229.0</MPVersio
n>
<MPToken
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">31bf3856ad364e35</MP
Token>
]]>
</Property>
      </Object>

      <Object
Path="$Context/Path[Relationship='LFX!System.LinkingFramework.ConnectorEmbedsCollections'
SeedRole='Source' TypeConstraint='LFX!System.LinkingFramework.DataCollection']$">
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollection
Name$">Sample_SMS_BIOS_CONSUMER_COLLECTION</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">S
ample_SMS_BIOS_CONSUMER_VIEW</Property>
        <Property
Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/Settings$"><![
CDATA[
```

```
<TypeName
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">HostedCustomClass</T
ypeName>
<MPName
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">SampleBIOSMP</MPName
>
<MPVersion
xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">1.0.0.0</MPVersion>
        ]]>
        </Property>
      </Object>
    </ObjectTemplate>
  </Templates>
</ManagementPack>
```

Importing Runbooks from System Center Orchestrator 2012

System Center 2012 – Service Manager integrates with System Center 2012 - Orchestrator, providing the capability to synchronously invoke runbooks from within Service Manager through the use of workflows. This capability provides integration between Orchestrator automation capabilities with the Self-Service Portal, as well as business modeling capabilities. When this capability is combined with the Service Manager Service Catalog stack, it is possible to create an end-user-facing request offering with an Orchestrator runbook as part of the fulfillment process.

Activities that make up a service request can be mapped to runbook activities, which in turn are mapped to an Orchestrator runbook. For example, the parameters that are necessary for a custom start activity to invoke a runbook in Orchestrator, such as a computer name, can go into as Service Manager as objects. You start this process by importing runbook objects into the Service Manager database using an Orchestrator connector. After you import runbooks into Service Manager, they appear in the **Library** node in the Administration workspace.

Note

Make sure that you have installed the ADO.NET Data Services Update for .NET Framework 3.5 Service Pack 1 (SP1), as described in Microsoft Knowledge Base article 976127. For more information, see ADO.NET Data Services Update for .NET Framework 3.5 SP1 for Windows 7 and Windows Server 2008 R2.

Importing Runbook Topics

- How to Create an Orchestrator Connector

  Describes how to create an Orchestrator connector.
- How to Synchronize an Orchestrator Connector

Describes how to synchronize an Orchestrator connector.

- How to Disable and Enable an Orchestrator Connector

  Describes how to temporarily disable and then re-enable an Orchestrator connector.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Create an Orchestrator Connector

You can use the following procedures in System Center 2012 – Service Manager to create a connector for System Center 2012 - Orchestrator and then validate the creation of the connector.

To create an Orchestrator connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Orchestrator connector**.
4. Perform these steps to complete the Orchestrator Connector Wizard:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that **Enable this connector** is selected, and then click **Next**.
   c. On the **Connection** page, in the **Server Information** area, type the URL of the Orchestrator Web service.
      i. Type the URL of the Orchestrator Web service in the form of http://<computer>:<port>/Orchestrator2012/Orchestrator.svc, where <computer> is the name of the computer hosting the web service and <port> is the port number where the web service is installed. (The default port number is 81.)
   d. On the **Connection** page, in the **Credentials** area, either select an existing account or click **New**, and then do the following:
      i. In the **Run As Account** dialog box, in the **Display name** box, type a name for the Run As account. In the **Account** list, select **Windows Account**. Enter the credentials for an account that has rights to connect Orchestrator, and then click **OK**. On the **Connection** page, click **Test Connection**.

         Note
         Special characters (such as the ampersand [&]) in the **User Name** box are not supported.

      ii. In the **Test Connection** dialog box, make sure that the message "The connection to the server was successful" appears, and then click **OK**. On the

Connection page, click **Next**.

e. On the **Folder** page, select a folder, and then click **Next**.

f. On the **Web Console URL** page, type the URL for the Orchestrator web console in the form of http://<computer>:port (the default port number is 82), and then click **Next**.

g. On the **Summary** page, make sure that the settings are correct, and then click **Create**.

h. On the **Completion** page, make sure that you receive the message "Orchestrator connector successfully created," and then click **Close**.

To validate the creation of an Orchestrator connector

1. In the **Connectors** pane, locate the Orchestrator connector that you created.
2. Review the **Status** column for a status of **Finished Success**.

   Note
   Allow sufficient time for the import process to finish if you are importing a large number of runbooks.
3. In the Service Manager console, click **Library**.
4. In the **Library** pane, expand **Library**, and then click **Runbooks**.
5. Review the **Runbooks** pane, and note that your runbooks have been imported.

How to Synchronize an Orchestrator Connector

To ensure that the Service Manager database in System Center 2012 – Service Manager is up to date, the Orchestrator connector synchronizes with Service Manager on a daily basis. You can use the following procedures to synchronize the connector manually and validate that the connector synchronized.

To manually synchronize an Orchestrator connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Orchestrator connector that you want to synchronize.
4. In the **Tasks** pane, under the name of the connector, click **Synchronize Now**.

To validate that an Orchestrator connector synchronized

1. In the Service Manager console, click **Connectors**.
2. In the **Connectors** pane, examine the start time and finish time to determine when the synchronization process started and finished.

   Note

Synchronization events are also written to the Event log in the Applications and Services Logs/Operations Manager folder.

How to Disable and Enable an Orchestrator Connector

You can use the following procedures in System Center 2012 – Service Manager to disable or enable an Orchestrator connector and validate the status of the connector.

To disable an Orchestrator connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Orchestrator connector that you want to disable.
4. In the **Tasks** pane, under the connector name, click **Disable**.
5. In the **Disable Connector** dialog box, click **OK**.

To enable an Orchestrator connector

1. In the Service Manager console, click **Administration**, and then click **Connectors**.
2. In the **Connectors** pane, select the Orchestrator connector that you want to enable.
3. In the **Tasks** pane, under the connector name, click **Enable**.
4. In the **Enable Connector** dialog box, click **OK**.

To validate the status change of an Orchestrator connector

1. In the middle pane, locate the connector for which you have changed status, and then verify the value in the **Enabled** column.

Importing Data from System Center Virtual Machine Manager

You can import objects, such as VM templates, service templates, and storage classifications that are created in Virtual Machine Manager (VMM) into the Service Manager database by creating a Virtual Machine Manager connector. After you import these objects into the Service Manager database, you can use these objects, for example, when you create Request Offerings.

If, in your environment, your VMM server pushes discovery data to an Operations Manager server, you will want to create an Operations Manager CI connector. You must make sure that the VMM management pack, Microsoft.SystemCenter.VirtualMachineManager.2012.Discovery, is synchronized with the Service Manager management server. You can create the Operations Manager CI connector either before or after creating the Virtual Machine Manager connector.

Importing VMM Data Topics

- How to Create a Virtual Machine Manager Connector

  Describes how to create a Virtual Machine Manager connector.
- How to Synchronize a Virtual Machine Manager Connector

  Describes how to synchronize a Virtual Machine Manager connector.
- How to Disable and Enable a Virtual Machine Manager Connector

  Describes how to disable and enable a Virtual Machine Manager connector.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Create a Virtual Machine Manager Connector

Use the following procedures in System Center 2012 – Service Manager to create a System Center Virtual Machine Manager connector and validate the creation of the connector.

To create a System Center Virtual Machine Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, under **Connectors**, click **Create Connector**, and then click **Virtual Machine Manager connector**.
4. Complete these steps to complete the Virtual Machine Manager Connector Wizard:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **General** page, in the **Name** box, type a name for the new connector. Make sure that **Enable this connector** is selected, and then click **Next**.
   c. On the **Connection** page, in the **Server Information** area, type the same of the computer hosting Virtual Machine Manager (VMM).
   d. On the **Connection** page, in the **Credentials** area, either select an existing account or click **New**, and then do the following:
      i. In the **Run As Account** dialog box, in the **Display name** box, type a name for the Run As account. In the **Account** list, select **Windows Account**. Enter the credentials for an account that has rights to connect VMM, and then click **OK**. On the **Connection** page, click **Test Connection**.

         Note
         Special characters (such as the ampersand [&]) in the **User Name** box are not supported.

      ii. In the **Test Connection** dialog box, make sure that **The connection to the**

server was successful appears, and then click **OK**. On the **Connection** page, click **Next**.

e. On the **Summary** page, make sure that the settings are correct, and then click **Create**.

f. On the **Completion** page, make sure that you receive a “Virtual Machine Manager connector successfully created” message, and then click **Close**.

To validate the creation of a System Center Virtual Machine Manager connector

1. In the **Connectors** pane, locate the System Center Virtual Machine Manager connector that you created.
2. Review the **Status** column for a status of **Running**.

   Note
   Allow sufficient time for the import process to finish if you are importing a large number of virtual machines or clouds.

3. In the Service Manager console, click **Configuration Items**.
4. In the **Tasks** pane, click **Create Folder**.
5. In the Create New Folder Wizard, do the following:
   a. In the **Folder name** box, type a name for the folder. For example, type **Test**.
   b. In the **Management pack** area, make sure that an unsealed management pack of your choice is selected, and then click **OK**. For example, select **Service Catalog Generic Incident Request**.
6. In the **Configuration Items** pane, click the folder you just created. For example, click **Test**.
7. In the **Tasks** pane, click **Create View**.
8. In the Create View Wizard, do the following:
   a. On the **General** page, in the **Name** area, type a name for this view. For example, type **VMMTemplates**.
   b. In the **Management pack** area, make sure that an unsealed management pack of your choice is selected. For example, select **Service Catalog Generic Incident Request**.
   c. In the navigation pane of the wizard, click **Criteria**.
   d. In the **Advanced Search** area, click **Browse**.
   e. In the drop-down list (located to the right of the **Type to filter** box), select **All basic classes**.
   f. In the **Type to filter** box, type **virtual machine template**, click **Virtual Machine Template**, click **OK**, and then click **OK** to save and close the form.
9. In the **Configuration Items** pane, expand the folder you created, and then click the view you created. For example, expand **Test**, and then click **VMMTemplates**
10. In the **VMMTemplates** pane, you will see the Virtual Machine Manager templates that have been created.

How to Synchronize a Virtual Machine Manager Connector

To ensure that the Service Manager database is up to date, the Virtual Machine Manager connector synchronizes with Service Manager on a daily basis. You can use the following procedures in System Center 2012 – Service Manager to synchronize the connector manually and validate that the connector synchronized.

To manually synchronize a Virtual Machine Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Virtual Machine Manager connector that you want to synchronize.
4. In the **Tasks** pane, under the name of the connector, click **Synchronize Now**.

To validate that a Virtual Machine Manager connector synchronized

1. In the Service Manager console, click **Connectors**.
2. In the **Connectors** pane, examine the start time and finish time to determine when the synchronization process started and finished.

   Note
   Synchronization events are also written to the Event log in the Applications and Services Logs/Operations Manager folder.

How to Disable and Enable a Virtual Machine Manager Connector

You can use the following procedures in System Center 2012 – Service Manager to disable or enable a Virtual Machine Manager connector and validate the status of the connector.

To disable a virtual Machine Manager connector

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Connectors** pane, select the Virtual Machine Manager connector that you want to disable.
4. In the **Tasks** pane, under the connector name, click **Disable**.
5. In the **Disable Connector** dialog box, click **OK**.

To enable a virtual Machine Manager connector

1. In the Service Manager console, click **Administration**, and then click **Connectors**.

2. In the **Connectors** pane, select the Virtual Machine Manager connector that you want to enable.
3. In the **Tasks** pane, under the connector name, click **Enable**.
4. In the **Enable Connector** dialog box, click **OK**.

To validate the status change of a virtual Machine Manager connector

1. In the middle pane, locate the connector for which you have changed status, and then verify the value in the **Enabled** column.

Using a CSV File to Import Data into Service Manager

This section provides an overview and procedures for importing data and configuration items into System Center 2012 – Service Manager by using comma-separated value (CSV) files.

Using a CSV File to Import Data Topics

- About Importing Data from Comma-Separated Files into Service Manager

  Describes the data and format files necessary for importing data from CSV files by using the Import from CSV feature.
- How to Import Configuration Items from a CSV File

  Describes how to import data items contained in a CSV file.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Importing Data from Comma-Separated Files into Service Manager

Configuration items contained in a comma-separated value (.csv) file can be imported into the Service Manager database by using the Import from CSV File feature. This feature lets you to bulk-import instances of any class type or projection type that is defined in the Service Manager database. You can use this feature to:

- Create configuration item or work item instances from data stored in a tabular format.
- Bulk-edit existing database instances.
- Populate the Service Manager database by using data exported from an external database.
- Circumvent data entry through forms when many class instances must be created at the same time.

Note

In this release, importing many complex items—for example, 5,000 computer projections—could take an hour or more. During this time, Service Manager continues to function.

Two files are required to import a set of instances by using the Import from CSV File feature:

1. A data file that consists of a series of comma-delimited object instances. The data file must end with the .csv file name extension.
2. A format file that specifies the class type or projection type of the instances present in the data file. Every instance in the data file is assumed to be of this kind. The format file also specifies (1) the subset of properties and, for projections, specifies components. They are being imported for the indicated type, and (2) the order in which those properties appear as columns in the associated data file. The format file must have the same file name as the csv file that it describes, and it must end with the .xml file name extension.

Creating the Data File

For example, you receive a spreadsheet that contains information about computers that you want to import into the Service Manager database. The following is a sample of the first 10 computers in the spreadsheet.

Computer Name	IP Address	Domain Name
WG-Det-1	172.30.14.21	DETROIT
WG-Det-2	172.30.14.22	DETROIT
WG-Det-3	172.30.14.23	DETROIT
WG-Dal-1	172.30.14.24	DALLAS
WG-Dal-2	172.30.14.25	DALLAS
WG-Chi-1	172.30.14.26	CHICAGO
WG-Chi-2	172.30.14.27	CHICAGO
WG-Chi-3	172.30.14.28	CHICAGO
WG-Chi-4	172.30.14.29	CHICAGO
WG-Chi-5	172.30.14.30	CHICAGO

The first step is to convert the data in the table into a .csv file format. In the .csv file, you make the assumption that the first row is data, and not a header. Therefore, you remove the header line from the spreadsheet and save the results as **newcomputers.csv** as in the following example.

```
WG-Det-1, 172.30.14.21, DETROIT

WG-Det-2, 172.30.14.22, DETROIT

WG-Det-3, 172.30.14.23, DETROIT

WG-Dal-1, 172.30.14.24, DALLAS
```

```
WG-Dal-2, 172.30.14.25, DALLAS

WG-Chi-1, 172.30.14.26, CHICAGO

WG-Chi-2, 172.30.14.27, CHICAGO

WG-Chi-3, 172.30.14.28, CHICAGO

WG-Chi-4, 172.30.14.29, CHICAGO

WG-Chi-5, 172.30.14.30, CHICAGO
```

Creating the Format File

A format file is now created that is suited to import the rows that are contained in the **newcomputers.csv** file. The first step in writing the format file is identifying the class type or projection type that must be used for the instances in the .csv file. For more information about class type or projection types, see the blog post Using the CSV import feature and download the file CSVImport.docx.

For the type of data being imported, you find that the **Microsoft.Windows.Computer** class is the best suited for the object type and property set. Start by declaring the class of the object that is being imported:

```
<CSVImportFormat>

   <Class Type=”Microsoft.Windows.Computer”>

      …

   </Class>

</CSVImportFormat>
```

After scanning the list of available properties of the **Microsoft.Windows.Computer** class, select the following properties for each column in the .csv file.

Column 1	Principal Name
Column 2	IPAddress
Column 3	DomainDnsName

By using these properties, you construct the following format file. The properties are listed in the order in which they appear in the .csv file. You must save this file that has the same file name for the .csv file, but with an .xml file name extension.

```
<CSVImportFormat>

   <Class Type="Microsoft.Windows.Computer">

      <Property ID="PrincipalName"/>

      <Property ID="IPAddress"/>

      <Property ID="DomainDnsName"/>

   </Class>
```

```
</CSVImportFormat>
```

Save this file as **newcomputers.xml**.

See Also

How to Import Configuration Items from a CSV File

How to Import Configuration Items from a CSV File

Before you can import data from a comma-separated value (CSV) file in System Center 2012 – Service Manager, you have to create two files: a data file and a format file. For more information about how to create these files, see About Importing Data From Comma-Separated Files into Service Manager. You can use the following procedure to import the Newcomputers.csv file by using the Newcomputers.xml format file.

To import configuration items from a CSV file

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Connectors**.
3. In the **Tasks** pane, click **Import from CSV file**.
4. In the **Import Instances from CSV File** dialog box, do the following:
   a. Next to the **XML format file** box, click **Browse**, and then select the format file. For example, select **Newcomputers.xml**, and then click **Open**.
   b. Next to the **Data file** box, click **Browse**, and then select the data file. For example, select **Newcomputers.csv**, and then click **Open**.
5. In the **Import Instances from CSV File** dialog box, click **Import**.
6. In the **Import Instances from CSV File** dialog box, verify that the numbers next to **Items saved**, **Instances created in memory**, and **Instances committed to database** are equal to the number of rows in the data file, and then click **Close**.

You can use a Windows PowerShell command to complete this task. For information about how to use Windows PowerShell to import configuration items from a CSV file, see Import-SCSMInstance.

To validate the import of configuration items from a CSV file

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, expand **Computers**, and then click **All Windows Computers**.
3. In the **All Windows Computers** pane, verify that the computers in the CSV file are listed.

Configuration Items in System Center 2012 - Service Manager

Configuration items are a way to store information about services, computers, software, software updates, users and other undefined imported objects in the Service Manager database in System Center 2012 – Service Manager. You can then select configuration items when you submit forms, such as an incident form, a change request form, or a work item form.

A service is a special kind of configuration item that includes both technical and business data. It supports troubleshooting and impact analysis by showing critical dependencies, settings, and areas of responsibility to other configuration items. The key benefit of using services is that you can easily see when incidents affect configuration items because services are viewed as a map, or hierarchy, of items. A service also identifies service owners, key customers, and users. Because a service maps the relationships between configuration items and work items, you should use services to help manage work items.

You can use connectors to import a large number of configuration items from Active Directory Domain Services (AD DS), Microsoft System Center Configuration Manager 2007 Service Pack 1 (SP1), and Operations Manager 2007, or you can manually create single CIs. You can also use the Operations Manager CI connector to import distributed applications in Operations Manager as a service. For more information about importing configuration items, see About Importing Data from System Center Configuration Manager and About Importing Data from Active Directory Domain Services.

Note

When you open a view to display a large number of items—typically, more than 5,000—the view can take a few minutes to display complete results.

Configuration Items Topics

- Creating Configuration Items

  Describes how to manually create configuration items, how to create a server, and how to create a view for imported configuration items.
- Deleting Configuration Items

  Describes the two-step process required to delete configuration items.
- Managing Configuration Items

  Describes how to add, browse, and delete related configuration items and how to manually add a user.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager

- Operations Guide for System Center 2012 – Service Manager

Creating Configuration Items

This section provides an overview of configuration items, describes how to manually create computer configuration items, how to create a service, and how to create a view for imported configuration items in System Center 2012 – Service Manager.

Creating Configuration Item Topics

- About Creating Configuration Items

  Provides an overview of how to create configuration items.
- How to Manually Create Configuration Items

  Describes how to manually create computer configuration items.
- How to Create a Service

  Describes how to manually create a service from configuration items imported from connectors.
- How to Create a View for Imported Configuration Items

  Describes how to create a view to edit and examine configuration items in Service Manager that do not have associated forms.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Creating Configuration Items

Configuration items are a way to store information about services, computers, software, software updates, users, and other undefined imported objects in the Service Manager database in System Center 2012 – Service Manager. You can then select configuration items when you submit forms, such as an incident form, a change request form, or a work item form.

A service is a special kind of configuration item that includes both technical and business data. It supports troubleshooting and impact analysis by showing critical dependencies, settings, and areas of responsibility to other configuration items. The key benefit of using services is that you can easily see when incidents affect configuration items because services are viewed as a map, or hierarchy, of items. A service also identifies service owners, key customers, and users. Because a service maps the relationships between configuration items and work items, you should use services to help you manage work items.

You can use connectors to import a large number of configuration items from Active Directory Domain Services (AD DS), Microsoft System Center Configuration Manager 2007 Service Pack 1

(SP1), and Operations Manager 2007, or you can manually create single configuration items. You can also use the Operations Manager CI connector to import distributed applications in Operations Manager as a service. For more information about importing configuration items, see Using Connectors to Import Data into System Center 2012 - Service Manager.

How to Manually Create Configuration Items

You might have to create a configuration item to add computers that do not exist in Active Directory Domain Services (AD DS) and that are not managed by Microsoft System Center Configuration Manager 2007 with Service Pack 1 (SP1) to the System Center 2012 – Service Manager database.

Additionally, you might have to manually create a new user configuration item to be used in the **Affected User** box in incidents created by Operations Manager.

You can use the following procedures to manually create two computer configuration items. However, you can also use the same procedures to add software, printers, or software updates in Service Manager. After you add the two computers, you can identify them as a service.

To manually create a computer configuration item

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, and then expand **Computers**.
3. Click **All Windows Computers**. In the **Tasks** pane, under **Computers**, click **Create Computer**.
4. In the form that appears, create a configuration item for a computer, such as **Exchange01.woodgrove.com**. On the **General**, **Software**, and **Related Items** tabs, enter information about the computer.
5. Click **OK** to save the new configuration item.
6. Repeat step 3 through step 5 to create a second computer, such as **Exchange02.woodgrove.com**.

To manually create a user configuration item

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, and then click **Users**.
3. In the **Tasks** pane, under **Users**, click **Create User**.
4. On the **General** tab in the form, follow these steps:
   a. In the **First Name** box, type a first name. For example, for the user account that will be used to populate the **Affected User** box for all incidents created by Operations Manager, type **OMAlert**.
   b. In the **Last Name** box, type a last name. For example, for the user account that will be used to populate the **Affected User** box for all incidents created by Operations Manager, type **User**.
5. On the **Notification** tab, click **Add**, and perform the following for each notification

address that you want to add:

a. In the **User Notification** dialog box, in the **Notification address name** box, type a name you want to use for this notification.
b. In the **Notification address description** box, type a description you want to use for this notification.
c. In the **Delivery address for this notification channel** box, type the address you would use to deliver a notification. Typically, this would be an email address.
d. Click **OK**.

To validate the manually created configuration item

- Verify that the computer you added appears in the **Computers** pane.
- Verify that the user you added appears in the **Users** pane.

How to Create a Service

You can use the following procedures to create a service in System Center 2012 – Service Manager. You should create and define business services that are critical to your enterprise. When you create a service, you create service configuration items, you define their business data, and you define relationships to other configuration items.

In the first procedure, you manually create a service from configuration items that are already present in Service Manager. This is a simple example and requires little other than a few existing configuration items.

In the second procedure, you view an edit a distributed application that was imported from Operations Manager. The prerequisites for this example can be very complex, depending on the distributed applications that you have created in Operations Manager. The following are high-level steps needed to import distributed applications from Operations Manager into Service Manager as services:

1. In Operations Manager, export each management pack that contains a component for your distributed application. Ensure that you export all management pack dependencies.

   Note
   You might need to download management packs or install them from the installation folder of your Operations Manager Root Management Server.

2. In Service Manager, import the management pack that contains the distributed application and its dependences. A new, empty, business service should appear in Business Services in the Configuration Items workspace.
3. Browse to **Administration** and then **Connectors** and ensure that you refresh the list of management packs. Then, synchronize the Operations Manager configuration items connector. When synchronization is complete, the service components appear in the **Configuration Items** workspace under the business service.

Generally, you should construct service maps that are 3-5 levels deep. Components of a service map should vary from 5-20 at each level. However, the total number of components should not exceed few hundred. This recommendation depends on the complexity of the service map, but keeping the number of components lower that a few hundred still provides reasonable response times, as you navigate throughout service map tree view. While the service map tree view expansion is still in progress, even for larger tree structures, the Service Manager console remains responsive. Service maps are not designed to handle a large number of components; as a result, we recommend that you keep your service map tree structures small.

To manually create a service for an IT messaging application

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, and then expand **Business Services**.
3. Click **All Business Services**, and then in the **Tasks** pane, under **Business Services**, click **Create Service**.
4. In the form that appears, click the **General** tab. In the **Display Name** box, type the name of the service to create. For example, type **IT Messaging Service**.
5. In the **Classification** list, select **E-mail and Communication**. In the **Owned By Organization** box, type the person or organization that provides the service. For example, type **Exchange Team**.
6. In the **Priority** list, select **Medium**. In the **Status** list, select **In Service**.
7. Next to the **Service owner** box, click the ellipsis button (**…**). Select the user who owns the service.
8. Next to the **Service contacts** box, click **Add** to select and add users who are contacts for the service.
9. Next to the **Service customers** box, click **Add** to select and add users who are business unit customers of the service.
10. Next to the **Affected users** box, click **Add** to select and add users or groups who use the service.
11. Click the **Service Components** tab to define the items on which the service depends.
12. Click **Add Category**. In the **Choose Class** dialog box, select **Computers Group**, and then click **OK**.
13. Under **Service Components**, select **ComputersGroup**, and then click **Add Item**.
14. In the **Select Objects** dialog box, under **Filter by class**, select **Computer**. Next, select individual computers to add to the group, and then click **OK**. For example, add **Exchange01.woodgrove.com** and **Exchange02.woodgrove.com**.

    Note

    You can select only one object at a time. Do not attempt to add multiple objects.
15. In the tree, click **Service Components**, and then click **Add Category**. In the **Choose Class** dialog box, select **Other Components Group**, and then click **OK**.
16. In the tree, select **OtherComponentsGroup**, and then click **Add Item**. In the **Select**

Objects dialog box under **Filter by Class List**, select **Services**, and then select **Active Directory Topology Root**. Next, click **OK**.

17. Click the **Service Dependents** tab to define the items that use the service or that are external to the service. For example, define other configuration items or services that use the new service.
18. Click **OK** to save the new configuration item.

To view and edit a distributed application that was imported from Operations Manager

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, expand **Business Services**, and then click **All Business Services**.
3. In the **All Business Services** pane, click the distributed application that you created in Operations Manager.
4. In the **Tasks** pane, under the title of the distributed application, click **Edit**.
5. In the **Service Maps – <DistributedApplicationName>** dialog box, click the **Service Components** tab to view the items defined in the Operations Manager distributed application. Then, expand the **Service Components** tree three levels.
6. Select any configuration item, and then click **Open** to view or edit its properties.

To view dependent services

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, expand **Business Services**, and then click **All Business Services**.
3. Select the **<DistributedApplicationName>**. In the **Tasks** pane, under **DistributedApplicationName>**, click **Edit**.
4. In the form that appears, click the **Service Dependents** tab. Services that use the new service are listed. For example, **IT Messaging Service** appears in the list.
5. Click **OK**.

How to Create a View for Imported Configuration Items

You can use the following procedures in System Center 2012 – Service Manager to create a view for imported Microsoft SQL Server database configuration items and then view the items in a dynamically generated form.

You can view and edit items that were imported from a System Center Operations Manager configuration item (CI) connector. However, Service Manager does not have system-defined views or forms for some items. For example, Service Manager does not have a defined view for SQL Server databases, so you must manually create a view to see these configuration items. Although Service Manager does not have a predefined form for SQL Server databases or for

many other objects that you might have imported, you can still view any configuration item in a dynamically generated form (if you created a view for those items).

Before you use these procedures, make sure that you import the SQL Server management packs for Operations Manager 2007 and for Service Manager. Although these procedures rely on SQL Server databases imported from Operations Manager, you can use the same steps to view other imported configuration items that do not have system-defined views or forms.

To create a view for imported SQL Server database configuration items

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, and then click **All Windows Computers**.
3. In the **Tasks** pane, under **Computers**, click **Create View**.
4. In the **Create View** dialog box, on the **General** page, in the **Name** box, type a name for the new view. For example, type **SQL Server Databases**.
5. In the **Description** box, enter a description of the view you are creating. For example, type **This view displays SQL Server databases from Operations Manager**.
6. Expand the **Criteria** area. Next to **Search for objects of a specific class**, click **Browse**.
7. In the **Select a Class** dialog box, in the **View** list, select **All basic classes**.
8. In the **Search** box, type **SQL**, and then click the search button (blue magnifying glass).
9. In the **Class** list, select **SQL 2008 DB**, and then click **OK**.
10. Click the **Display** tab. In the **Columns to display** list, select **Database Name** and **Database Size (MB) String**, and then click **OK**.
11. Select the **SQL Server Databases** view to see the list of the imported SQL Server databases.

To view and edit imported SQL Server database configuration items

1. Select the **SQL Server Databases** view that you created, and then select any item in the list. Notice that the **Preview** pane shows detailed information about the selected item.
2. Double-click any item in the list to view the item in a dynamically generated form.
3. Optionally, you can edit various fields for the item in the same manner as you do for other configuration items.
4. Optionally, you can perform actions in the **Tasks** list, in the same manner as you do for other configuration items.
5. If you have made any changes to the item, click **OK**; otherwise, click **Cancel** to close the form.

You can use Windows PowerShell commands to display views that are defined in Service Manager. For more information, see Get-SCSMView.

Deleting Configuration Items

Deleting configuration items is a two-step process, and only members of the Advanced Operators, Authors, and Administrators user roles can initiate the Delete process in System Center 2012 – Service Manager. The first step does not delete configuration items directly. Instead, this process changes the property values of a configuration item so that the item will only be displayed in a **Deleted Items** view. The state of the configuration item is changed from Active to Pending Delete. A Service Manager administrator can later log on and permanently delete the configuration item from the Service Manager database.

Deleting Configuration Items Topics

- How to Initiate the Deletion of a Configuration Item

  Describes how to delete a configuration item.
- How to Delete or Restore a Configuration Item

  Describes how to permanently delete a configuration item.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Initiate the Deletion of a Configuration Item

You can use the following procedures to initiate the deletion of a configuration item in System Center 2012 – Service Manager and validate the initiation of the deletion. Only users who are members of the Advanced Operators, Authors, or Administrators user role can initiate the deletion of a configuration item. Only users who are members of the Administrators user role can complete the deletion of a configuration item.

To initiate the deletion of a configuration item

1. Log on to a computer that hosts the Service Manager console by using a user account that is a member of the Advanced Operators, Authors, or Administrators user role.
2. In the Service Manager console, click **Configuration Items**.
3. In the **Configuration Items** pane, expand **Configuration Items**, expand **Computers**, and then click **All Windows Computers**.
4. In the **All Windows Computers** pane, click the computer to be deleted.
5. In the **Tasks** pane, under the name of the computer that you selected in the previous step, click **Delete**.
6. In the **Delete Item** dialog box, confirm your selection, and then click **Yes**.

To validate that the deletion of a configuration item has been initiated

1. In the Service Manager console, click **View**, and then click **Refresh**. Or, press F5.
2. Verify that the configuration item you selected is no longer displayed.

   Note
   At this point, the configuration item has been moved to a **Deleted Item** view that is only available to members of the Administrator user role. An administrator must permanently delete the configuration item.

You can use Windows PowerShell commands to complete these tasks, as follows:

- For information about how to use Windows PowerShell to initiate the deletion of a configuration item by updating the `PendingDelete` property value, see Update-SCSMClassInstance.
- For information about how to use Windows PowerShell to retrieve items that have been marked for deletion in Service Manager, see Get-SCSMDeleteditem.

See Also

How to Delete or Restore a Configuration Item

How to Delete or Restore a Configuration Item

After members of the Advanced Operators, Authors, or Administrators user roles have initiated the deletion of a configuration item, a System Center 2012 – Service Manager administrator can use the following procedures to either permanently delete the configuration item or to restore the original properties for this item. You may need to refresh the Service Manager console to update the list of configuration items.

To complete the deletion of a configuration item

1. Log on to a computer that hosts the Service Manager console by using a user account that is a member of the Administrators user role.
2. In the Service Manager console, click **Administration**.
3. In the **Administration** pane, expand **Administration**, and then click **Deleted Items**.
4. In the **Deleted Items** pane, click the configuration items that you want to permanently delete. You can use the CTRL or SHIFT keys to select multiple configuration items.
5. In the **Tasks** pane, click **Remove Items**.

   Note
   For this release, if you are logged in as an administrator, you will see three options in the **Tasks** pane under the name of the computer: **Delete**, **Remove Items**, and **Restore Items**. In the **Deleted Items** view, select only **Remove Items** or **Restore Items**.
6. In the **System Center Service Manager** dialog box, make sure you selected the correct

items, and then click **Yes**.

To restore a configuration item

1. Log on to a computer that hosts the Service Manager console by using a user account that is a member of the Administrators user role.
2. In the Service Manager console, click **Administration**.
3. In the **Administration** pane, expand **Administration**, and then click **Deleted Items**.
4. In the **Deleted Items** pane, click the configuration items that you want to restore to the Service Manager database. You can use the CTRL or SHIFT keys to select multiple configuration items.
5. In the **Tasks** pane, click **Restore Items**.

   Note
   For this release, if you are logged in as an administrator, you will see three options in the **Tasks** pane under the name of the computer: **Delete**, **Remove Items**, and **Restore Items**. In the **Deleted Items** view, select only **Remove Items** or **Restore Items**.
6. In the **Delete Item** dialog box, make sure that you selected the correct items, and then click **Yes**.

You can use Windows PowerShell commands to complete these tasks, as follows:

- For information about how to use Windows PowerShell to permanently remove an instance of a configuration item object, see Remove-SCSMClassInstance.
- For information about how to use Windows PowerShell to restore items that were previously marked for deletion in Service Manager, see Restore-SCSMDeleteItem.

See Also

How to Initiate the Deletion of a Configuration Item

Managing Configuration Items

You might want to associate the work item to apply the Microsoft Exchange Server 2010 with Service Pack 1 (SP1) update to the service that represents the computers that are affected by the email incident. To accomplish this, you can update the service configuration item and then add the respective work item as a related item.

Managing Configuration Item Topics

- How to Add, View, or Remove Related Configuration Item Information

  Describes how to add, browse, or delete related configuration item information.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager

- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Add, View, or Remove Related Configuration Item Information

You can use the following procedures to add information, such as related work items or files, to configuration items in System Center 2012 – Service Manager. The procedures in this topic describe only how to add items, but you can follow similar steps to view or remove items.

For example, when you are troubleshooting an incident, you might discover that a relationship exists between two or more objects. A work item to apply an application service pack might be related to more than one configuration item. You might need to update the configuration items to reflect that relationship.

Similarly, work items such as incidents, problems, and change requests are often interrelated. Related work items share some commonality with each other or with a configuration item. When a work item affects a particular configuration item, they are linked.

To add information to configuration items

1. In the Service Manager console, click **Configuration Items**.
2. In the **Configuration Items** pane, expand **Configuration Items**, and then expand **Computers**.
3. Click **All Windows Computers**. In the **All Windows Computers** pane, double-click the computer to which you want to add information.
4. In the computer form, click the **Related Items** tab.

To add related services, people, and configuration items

a. In the **Configuration Items: Computers, Services, and People** area, click **Add**.
b. In the **Select Objects** dialog box, select a class from the **Filter by class** list to narrow the choices available in the **Available objects** list.
c. In the **Available objects** list, select the items that you want to add, and then click **Add**.
d. Click **OK** to close the dialog box and to add the selected items.

To add related work items

a. In the **Related work items** area, click **Add**.
b. In the **Select Objects** dialog box, select a class from the **Filter by class** list to narrow the choices available in the **Available objects** list.
c. In the **Available objects** list, select the work items that you want to add, and then click **Add**.

d. Click **OK** to close the dialog box and to add the selected work items.

To attach files

a. In the **Attached files** area, click **Add**.
b. In the **Open** dialog box, select the file that you want to add, and then click **Open**.
c. In this release, do not attempt to open an attached file before you submit the form.

5. Click **OK** to save the form.

Configuring Incident Management in System Center 2012 - Service Manager

This section provides an overview of how to configure incident management in System Center 2012 – Service Manager. This section also contains procedures that cover incident management configuration scenarios, including configuring incident settings, configuring email incident support, and creating an incident template.

Configuring Incident Management Topics

- About Configuring Incident Management in Service Manager

  Provides an overview of how to configure incident management.
- How to Set File Attachment Limits

  Describes how to set the number of files and the size of a file that can be attached to an incident.
- How to Set Parent Incident Options

  Describes how to set parent and child default actions for automatic resolution, automatic reactivation, and automatic incident status updates.
- How to Set Incident Priority

  Describes how to define the incident priority based on impact and urgency.
- How to Set Resolution Time

  Describes how to define the incident resolution time based on incident priority.
- How to Set Operations Manager Web Settings

  Describes how to specify the URL that Service Manager uses to connect to the Operations Manager 2007 web console.
- How to Configure Your Infrastructure for Email Incident Support With Exchange Server 2007

Describes how to configure Exchange Server 2007 and Simple Mail Transfer Protocol (SMTP) to let users submit incidents by sending email.

- How to Configure Your Infrastructure for Email Incident Support With Exchange Server 2007

  Describes how to configure Exchange Server 2010 and Simple Mail Transfer Protocol (SMTP) to let users submit incidents by sending email.

- How to Create Incident Templates

  Describes how to create a template that is used when you create incidents.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Configuring Incident Management in Service Manager

Several features in System Center 2012 – Service Manager let you streamline the creation of incidents. You can configure incident settings such as the following in Service Manager:

- Priority calculations that are based on impact and urgency
- Target resolution time
- Prefixes that are used for incident numbers
- Length of time a closed incident remains in the Service Manager database

You can create an incident template to populate certain fields for a specified incident type, such as email-related problems. Help desk personnel use templates when creating incidents. The template prepopulates some of the fields in the incident, such as the name of the support analyst who handles email-related problems.

You can configure incident management to automatically generate incidents based on desired configuration management for configuration items that are not in compliance. This works only if Microsoft System Center Configuration Manager 2007 Service Pack 1 (SP1) with desired configuration management baselines is installed in your environment.

The procedures in this section describe how to configure incidents. You can define incident priority based on impact and urgency, specify resolution times based on incident priority, create an incident template, and create a new incident based on desired configuration management.

Configuring Incident Settings

You can use the procedures in this section to configure settings for incident number prefixes, file attachment limits, incident priority calculations, resolution times, and System Center Operations Manager Web settings.

In System Center 2012 – Service Manager, all incident numbers start with "IR". However, you can change the prefix that is used for your incident numbers.

The policy at your organization might limit the number of files that can be attached to each incident to no more than five and to limit the maximum file size for each file at 500 kilobytes (KB).

Note

The maximum number of attached files and maximum file size settings that you configure also apply to the attached files in the **Related Items** tab for configuration items.

Incident priority calculation is rated on a scale from 1 to 9. A priority of 1 is the highest priority. It is based on a combination of impact and urgency. Impact and urgency settings are defined as High, Medium, or Low, and they are configured when the incident is created. The following table shows how to define the incident priority for each possible combination of impact and urgency.

Priority Calculation Table

		Impact		
		Low	Medium	High
Urgency	Low	9	8	7
	Medium	6	5	4
	High	3	2	1

The resolution time defines how much time it should take to resolve an incident. Resolution time is based on priority. Typically, you should set resolution times for higher-priority incidents. The procedures in this section describe how to set the values for file attachments, incident priority, and resolution time.

You can create a connector to import alerts and configuration items fromOperations Manager. By using the Operations Manager alert connector, Service Manager can create incidents based on alerts. When you view these incidents in Service Manager, you can click a link to obtain more information about the alert or about the health state of the configuration item. Service Manager uses the Operations Manager Web console server to provide this information. Service Manager uses the URL that you specify in the Operations Manager Web setting to connect to Operations Manager.

Creating an Incident Template

You can use the procedures in this section to create incident templates in System Center 2012 – Service Manager for problems that are, for example, related to email and printers.

When an analyst at the help desk receives a call, there are many pieces of information that the analyst must gather to create an incident, such as a summary of the problem; the name of the user to whom the incident will be assigned; the impact; the urgency; and whether this is a Tier 1, 2, or 3 incident. For some systems in the enterprise, this information might already be known.

For example, if a problem occurs with the e-mail system, the incident is classified as high-impact and high-urgency, handled at a Tier 2 level, and assigned to a specific analyst. You can create an

incident template that, when it is applied to a new incident form, populates many fields in the new incident. This reduces the required time to create an incident, and it ensures accuracy and consistency.

Incident templates are also used as part of the Incident Change workflow. For example, your company might have determined that if the urgency of a printer-related problem changes from Low to High, that incident should automatically be elevated to the Tier 2 level.

You can use the procedures in this section to create two incident templates, one to create email-related incidents and another to use with the Incident Change workflow for printer-related problems.

Configuring Incident Support Through Email

Instead of placing a call to the help desk, your end-users can submit incidents by sending an email message to a dedicated email address. Several email addresses can be used, one for hardware, one for software, and one for printers. For example, when a message is sent to Helpdesk@Helpdesk.Woodgrove.com, Microsoft Exchange Server copies the message to a "drop folder" on the computer that is hosting an SMTP Server service. Service Manager monitors this share and processes the message into an incident. Service Manager parses the **From** address and attempts to match the user in the Service Manager database. If Service Manager cannot find the user in the Service Manager database, the message is moved into a "bad folder", and no incident is created. An administrator monitors the "bad folder".

The infrastructure that is required to handle incidents generated by email includes an existing server running Exchange Server or an SMTP Server and a new server that runs the SMTP service for Service Manager. For this new server, use Internet Information Services (IIS) 6.0 SMTP services (which is included with Windows Server 2008) on either the computer that is hosting the Service Manager management server or on a separate remote server.

Delegate one of the existing servers that is running Exchange Server or SMTP Server in your enterprise to route all email messages addressed to the help desk, and then configure the IIS SMTP service for use with Service Manager. Providing precise instructions for various versions of Exchange Server or SMTP Service is beyond the scope of this guide. For more information about how to set up Simple Mail Transfer Protocol (SMTP) domains for incoming and relay email, see article 260973 in the Microsoft Knowledge Base.

How to Set File Attachment Limits

Use the following procedure to limit the number and size of files that can be attached to an incident in System Center 2012 – Service Manager. In this example, set the maximum number of files to 5 and the maximum file size to 500 kilobytes (KB).

To set file attachment limits

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.

3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, click **General**.
6. Set **Maximum number of attached files** to **5**.
7. Set **Maximum size (KB)** to **500**, and then click **OK**.

To validate file attachment limits

- When you create a new incident or edit an existing one, no more than five files can be attached, and each file can be no larger than 500 KB.

How to Set Parent Incident Options

Use the following procedure to set default options for parent and child incidents in System Center 2012 – Service Manager. The default options determine whether child incidents automatically resolve, whether child incidents automatically activate, and whether child incident status automatically updates.

When choosing to automatically resolve child incidents or automatically reactivate child incidents when its parent is resolved or when its parent is reactivated, you can prompt the resolving analyst for their decision. When prompted, an analyst can choose a resolution category or activation status. Otherwise, when incidents are automatically resolved or activated, the analyst is not prompted and the changes are effectively immediately using the parent incident settings.

To automatically resolve child incidents

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, click **Parent Incident** and then choose one of the following actions:
   - If you want to automatically resolve a child incident when its parent is resolved without any analyst interaction, set **Auto resolution of child incidents** to **Automatically resolve child incidents when parent incident is resolved**, and then choose either **Same as parent incident category** or **Choose a child incident category** and a default resolution category.
   - If you want to automatically resolve a child incident when its parent is resolved and have an analyst review and verify the incident resolution category, select **Auto resolution of child incidents** to **Let the analyst decide when resolve the parent incident** and then choose either **Same as parent incident category** or **Choose a child incident category** and a default resolution category.
   - If you do not want child incidents to automatically resolve, select **Auto resolution of**

child incidents to **Do not resolve child incidents when parent incident is resolved**.

6. Click **OK**.

To automatically activate child incidents

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, click **Parent Incident**, and then choose one of the following actions:
   - If you want to automatically activate a child incident when its parent is activated without any analyst interaction, set **Auto reactivation of child incidents** to **Automatically reactivate child incidents when parent incident is reactivated**, and then choose a default reactivation status.
   - If you want to automatically resolve a child incident when its parent is resolved and have an analyst review and verify the incident reactivation status, select **Auto reactivation of child incidents** to **Automatically reactivate child incidents when parent incident is reactivated**, and then choose a default reactivation status.
   - If you do not want to automatically activate child incidents, set **Auto reactivation of child incidents** to **Do not reactivate child incidents when parent incident is reactivated**.
6. Click **OK**.

To automatically update child incident status

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, click **Parent Incident**, and then choose one of the following actions:
   - If you want to automatically update child incident status when it is linked to a parent incident, set **Status of active child incidents when linked to parent** to **Automatically change the status of active child incidents when linking to parent**, and then choose an available incident status.
   - If you do not want to automatically update child incident status, set **Status of active child incidents when linked to parent** to **Do not change the status of child incidents**.
6. Click **OK**.

How to Set Incident Priority

Use the following procedure in System Center 2012 – Service Manager to define a priority calculation table based on impact and urgency settings that are defined during the creation of an incident.

To set incident priority

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, select **Priority Calculation**.
6. For each of the High, Medium, and Low settings for both impact and urgency, select an incident priority value from 1 through 9, and then click **OK**.

To validate incident priority

- When you create a new incident or edit an existing one, the resulting priority setting must match the value that is entered in the table for a specific High, Medium, and Low setting that is defined for impact and urgency.

How to Set Resolution Time

Use the following procedure to set a resolution time based on incident priority in System Center 2012 – Service Manager.

To set resolution time

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, select **Resolution Time**.
6. For each of the priority settings of 1 through 9, specify the amount of time for incident resolution.
7. Click **OK**.

To validate resolution time

- When you create a new incident or edit an existing one, the resulting resolution times for an incident matches the values that are defined in the preceding procedures.

How to Set Operations Manager Web Settings

Use the following procedures to set the web settings of System Center Operations Manager 2007 in System Center 2012 – Service Manager and validate the settings.

To set Operations Manager web settings

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Incident Settings**.
4. In the **Tasks** pane, under **Incident Settings**, click **Properties**.
5. In the **Incident Settings** dialog box, click **Operations Manager Web Settings**.
6. In the **Web Console URL** box, type the URL of the Operations Manager 2007 web console server, and then click **OK**. For example, type **http://<servername>:51908**, where <servername> is the name of the computer hosting the web console server.

To validate Operations Manager web settings

- Make sure that you can access the web console server by entering **http://<servername>:51908** into your browser, where <servername> is the name of the computer hosting the web console server.

How to Configure Your Infrastructure for Email Incident Support With Exchange Server 2007

Use the following procedures to configure your infrastructure to support the creation of incidents through email.

To configure Exchange 2007 to route email messages

1. Open the **Exchange Management** console.
2. Expand **Organization Configuration**, and then click **Hub Transports**.
3. In the **Hub Transport** pane, click **Accepted Domain**.
4. In the **Actions** pane, click **New Accepted Domains**.
5. In the **New Accepted Domains** dialog box, create a new accepted domain of the type **Internal Relay**. In this example, you might specify the domain as ***.Helpdesk.Woodgrove.com**.
6. In the **Hub Transport** pane, click **Send Connectors**.
7. In the **Actions** pane, click **New Send Connector**.
8. In the New SMTP Send Connector Wizard, create a new send connector by using the following information:
   a. Address space = *.Helpdesk.Woodgrove.com
   b. Add Smart Host by using the IP address of the computer that will host the SMTP

Server service defined in the following procedure.

c. Set **smart host authentication settings** to **None**.

To configure the IIS SMTP Server service for Service Manager

1. On the computer that will host the SMTP Server service, on the taskbar, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) 6.0 Manager**.
2. Right-click the **Local Computer** node, click **New**, and then click **SMTP Virtual Server**.
3. In the New SMTP Virtual Server Wizard, in the **Name** box, type the name for the Simple Mail Transfer Protocol (SMTP) server, and then click **Next**. For example, type **Helpdesk.Woodgrove.com**.
4. On the **Select IP Address** page, click the drop-down list and select the IP address of the computer that is hosting the SMTP Server, and then click **Next**.
5. On the **Select Home Directory** page, click **Browse**, and then click the folder for your home directory. For example, select **C:\inetpub\mailroot**. You will create a share for this folder in the next procedure.
6. On the **Default Domain** page, type the domain name for this virtual SMTP server, and then click **Finish**. The domain name that you enter must match the domain name from step 3 in the previous procedure. For example, type **Helpdesk.Woodgrove.com**.

To create a share for the mail root folder

1. On the taskbar, click **Start**, and then click **Explore**.
2. In Windows Explorer, browse to the folder that you specified as the home directory in step 5 from the previous procedure. For example, browse to **C:\Inetpub\Mailroot**. If needed, create two subfolders, **Badmail** and **Drop**.
3. Right-click the home folder, and then click **Share**.
4. In the **File Sharing** dialog box, select the domain user that you specified for the Service Manager account, click **Contributor**, click **Share**, and then click **Done**.
5. Make sure that the **Simple Mail Transfer Protocol (SMTP)** service is set to **Automatic** and has started.

To configure incoming Email settings in Service Manager

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, double-click **Incident Settings**.
4. In the **Incident Settings** dialog box, click **Incoming E-mail**.
5. In the **SMTP Service drop folder location** box, type the path, share, and folder to the Drop folder. In this example, type **\\<computer_name>\mailroot\Drop**, where <computer_name> is the name of the computer that is hosting the SMTP Server service, Mailroot is the share name, and Drop is the subfolder.
6. In the **SMTP Service bad folder location** box, type the path, share, and folder to the

Badmail folder. In this example, type **\\<computer_name>\Mailroot\Badmail**, where <computer_name> is the name of the computer that is hosting the SMTP Server service, Mailroot is the share name, and Badmail is the subfolder.

7. In the **Maximum number of e-mails to process at a time** box, enter a number for the email messages that you want Service Manager to process during an email processing cycle.
8. Select the **Turn on incoming e-mails processing** check box, and then click **OK**.

How to Configure Your Infrastructure for Email Incident Support with Exchange Server 2010

Use the following procedures to configure your Microsoft Exchange Server 2010 infrastructure to support the creation of incidents through email.

To install and configure the SMTP server

1. Log on with administrative credentials on the server that will host the Simple Mail Transfer Protocol (SMTP) server role.

   Note
   A server running Exchange Server 2010 cannot be your SMTP server.
2. Click **Start**, navigate to **All Programs**, **Administrative Tools**, and then click **Server Manager**.
3. In Server Manager, click **Features**, and in the **Features** pane, click **Add Features**.
4. In the **Select Feature** window, click **SMTP Server**.
5. The Add Features Wizard appears. If the dependent role services are not already selected, you are prompted to add role services and features for the SMTP server. Click **Add Required Role Services**.
6. On the **Select Features** page, click **Next**.
7. On the **Web Server (IIS)** page, click **Next**.
8. On the **Select Role Service** page, click **Next**.
9. On the **Confirm Installation Selections** page, click **Install**.
10. When the **Installation Results** page appears, click **Close** to exit the wizard.

To configure the IIS SMTP server service for Service Manager

1. On the server that is hosting the SMTP server service, open **Administrative Tools**, and then click **Internet Information Services (IIS) 6.0 Manager**.
2. Expand the SMTP server until you see **SMTP Virtual Server #1**. The SMTP server might have a different name, but it appears with an email icon.
3. Right-click **SMTP Virtual Server #1**, click **Rename**, and then type the name of your server.

4. Expand **Domains**, and then rename the domain to the fully qualified domain name (FQDN) of the server or the domain name that you want to use.

   Note
   This cannot be the same domain that the server is a member of. However, it can be a child domain.

   For example, if the domain name is contoso.com, you use a server name that resembles server.contoso.com.
5. Using the server name from step 3, right-click the server name, and then click **Properties**.
6. Click the **Access** tab, and then click **Relay**.
7. On the **Relay Restrictions** tab, click **All except the list below**, click **Allow all computers which successfully authenticate to relay regardless of the list above**, and then click **OK**.
8. Click the **Delivery** tab, and then click **Advanced**.
9. In the **Advanced Delivery** window, type the values as shown here:
   a. For **Masquerade Domain**, type your root domain name, for example, **contoso.com**.
   b. For the FQDN, type your Exchange server name, for example, **exchange.contoso.com**.
   c. For **Smart host**, type your Exchange server name, for example, **exchange.contoso.com**.
   d. Click **OK**, and then click **OK** again to close the **Advanced Delivery** window.
10. Close IIS 6.0 Manager, open Windows Explorer, and navigate to <SystemDrive>:\Inetpub\Mailroot.
11. Create two child folders. Name the first folder **Badmail**, and name the second folder **Drop**.
12. Right-click the <SystemDrive>:\Inetpub\Mailroot folder, and then click **Share**.
13. For sharing permissions, select the domain user that you specified for the Service Manager account, click **Contributor**, click **Share**, and then click **Done**.
14. Restart the Simple Mail Transfer Protocol (SMTP) service, ensure that it is set to **Automatic**, and verify that it has started.

To configure Service Manager for email

1. Open the Service Manager console, and then select **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, double-click **Incident Settings**.
4. Scroll to **Incoming E-mail**.
5. In **The SMTP Service drop folder location**, type the path, share, and folder for the Drop folder. In this example, type **\\<computer_name>\mailroot\Drop**, where **<computer_name>** is the name of the computer that is hosting the SMTP Server service, **Mailroot** is the share name, and **Drop** is the subfolder name.

6. In **SMTP Service bad folder location**, type the path, share, and folder to the Badmail folder. In this example, type **\\<computer_name>\Mailroot\Badmail** where **<computer_name>** is the name of the computer that is hosting the SMTP Server service, **Mailroot** is the share name, and **Badmail** is the subfolder name.
7. In **Maximum number of e-mails to process at a time**, type a number for the emails that you want Service Manager to process during an email processing cycle.
8. Select **Turn on incoming e-mails processing**, and then click **OK**.

To configure email notifications

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Notifications**, and then click **Channels**.
3. In the **Channels** pane, click **E-Mail Notification Channel**.
4. In the **Tasks** pane, under **E-Mail Notification Channel**, click **Properties** to open the **Configure E-Mail Notification Channel** dialog box.
5. Click **Enable e-mail notifications**, and then click **Add**.
6. In the **Add SMTP Server** dialog box, type the FQDN of the SMTP server that you want to use. For example, type **Servername.domain.com**.
7. In **Port number**, type or select the SMTP port number that you want to use. For example, select **25**.
8. Click **Add**, and in the **Add SMTP Server** dialog box, type the FQDN of the SMTP server that you want to use. For example, type **Exchange.domain.com**, and replace the information with your Exchange domain name information.
9. In **Port number**, type or select the SMTP port number that you want to use. For example, select **25**.
10. In **Authentication method**, click **Anonymous**, and then click **OK**.
11. In **Return e-mail address**, type the email address of the service account that was used during Setup. For example, type **Helpdek@Servername.domain.com**.
12. In **Retry primary after**, type or select the number of seconds that you want Service Manager to wait before trying to resend outgoing email notifications. For example, select **25**.
13. Click **OK** to close the dialog box.

To validate email notification configuration

1. In the **Channels** pane, **click E-Mail Notification Channel**.
2. In the **Tasks** pane, under **E-Mail Notification Channel**, click **Configure** to open the **Configure E-Mail Notification Channel** dialog box.
3. Confirm that the configuration you entered is correct.

Configuring Exchange 2010 for use with Service Manager

In the following procedures, you configure Exchange 2010 for use with Service Manager. You perform these procedures on the server that hosts Exchange Server 2012.

To configure the Organization Hub Transport

1. In Exchange Server, click **Organization Configuration**, and then click **Hub Transport**.
2. In the **Hub Transport** window, click the **Accepted Domains** tab.
3. In the **Actions** pane, click **New Accepted Domain**.
4. In the New Accepted Domain Wizard, on the **New Accepted Domain** page, in the **Name** box, type a descriptive name. For example, type **From SMTP Server**, and in **Accepted Domain**, type the SMTP domain name that you created for Service Manager. For example, type ***.Servername.domain.com**.
5. Click **Authoritative Domain**, and then click **New**.

To configure the Server Configuration Hub Transport

1. In Exchange Server, navigate to **Server Configuration**, and then click **Hub Transport**.
2. In the **Actions** pane, click **New Receive Connector** to open the New Receive Connector Wizard.
3. In **Name**, type a name that identifies the Service Manager SMTP server, select **Custom** for the intended use, and then click **Next**.
4. On the **Local Network Settings** page, accept the default value, leave the **FQDN** box empty, and then click **Next**.
5. On the **Remote Network Settings** page, remove the existing IP address, type the IP address of your Service Manager SMTP server, and then click **Next**.
6. On the **New Connector** page, click **New** to complete the wizard.
7. Double-click the newly created **Receive Connector** to open its properties, click the **Authentication** tab, and then clear any items that are selected.
8. Click the **Permissions Groups** tab, click **only Anonymous users**, and then click **OK**.
9. To grant relay permission to anonymous connections on the new receive connector, open **Exchange Management Shell**, type the following, and then press ENTER:

```
Get-ReceiveConnector "Anonymous Relay" | Add-ADPermission -
User "NT AUTHORITY\ANONYMOUS LOGON" -ExtendedRights "Ms-Exch-
SMTP-Accept-Any-Recipient"
```

10. Close Windows PowerShell.

To configure the mail contact in Exchange

1. In Exchange Server, navigate to **Recipient Configuration**, and then click **Mail Contact**.
2. In the **Action** pane, click **New Mail Contact**.

3. In the New Mail Contact Wizard, click **New contact**, and then click **Next**.
4. In **Name**, type the name that you want to use as the Service Manager return email address, without @domain.com. For example, type **Helpdesk**.
5. In **Alias**, type the name that you want users to use as the **Email Alias** name. For example, type **Helpdesk**.
6. Edit the **External e-mail address**, and type the FQDN for the email address. For example, type **helpdesk@server.domain.com**.
7. Click **Next**, and then click **New** to complete the wizard.

To test email functionality between the SMTP server and the Exchange server

1. Using Windows Explorer on the SMTP server, create a new text file named **TESTEMAIL**.
2. Remove the TXT file name extension from the new file.
3. Right-click the TESTMAIL file, and then click **Open**.
4. When you are prompted to open the file with a program, click **Notepad**, and then click **OK**.
5. In the file, type the following using your own information, similar to the following example:

```
to:username@domain.com

from:Helpdesk@servername.domain.com

Subject:This is an email test.

This is a test
```

6. Save the file without a file name extension, and then close Notepad.
7. Copy the file to a location where you can use it in the future for testing.
8. Copy the file into the <SystemDrive>:\inetpub\mailroot\Pickup folder.

   Note
   The file should be removed automatically. This indicates that the Exchange server is using it.
9. Using the user credentials for the **To** recipient that you typed previously, open Outlook and confirm that the email was received.

How to Create Incident Templates

Use the following procedures to create two incident templates in System Center 2012 – Service Manager. The first you use to create email-related incidents, and the second you use with the Incident Change workflow for printer-related problems.

To create an email-related incident template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Templates**.

3. In the **Tasks** pane, in the **Templates** area, click **Create Template**.
4. In the **Create Template** dialog box, complete these steps:
   a. In the **Name** box, type a name for the incident template. For example, type **E-mail Incident**.
   b. In the **Description** box, type a description for the incident template. For example, type **Use this template to start all email-related incidents**.
   c. Click **Browse** to choose a class.
   d. In the **Choose Class** dialog box, click **Incident**, and then click **OK**.
   e. In the **Management Pack** list, select **Service Manager Incident Management Configuration Library**, and then click **OK**.
5. In the incident template form, complete these steps:
   a. Leave the **Affected user** box empty.
   b. Leave the **Alternate contact information** box empty. Alternate contact information for the affected user is entered when the incident is created.
   c. In the **Title** box, type a title for the template. Or, type a preface, such as **Email:**.
   d. In the **Classification Category** box, select the category that reflects the problem to report. For example, select **E-mail Problems**.
   e. Leave the **Source** box empty. The **Source** box is automatically populated when the incident is created.
   f. In the **Impact** box, select a value. For example, select **High**.

      In the **Urgency** box, select a value. For example, select **High**.
   g. In the **Support Group** box, select a tier. For example, if you want all email-related issues to be assigned to the tier 2 support group, select **Tier 2**.
   h. Click **OK**.

To create a new printer-related incident template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Templates**.
3. In the **Tasks** pane, click **Create Template**.
4. In the **Create Template** dialog box, complete these steps:
   a. In the **Name** box, type a name for the incident template. For example, type **Escalate Printer Problems to Tier 2**.
   b. In the **Description** box, type a description for the incident template. For example, type **Use this template to assign high-urgency printer-related problems to tier 2**.
   c. Click **Browse** to choose a class.
   d. In the **Choose Class** dialog box, click **Incident**, and then click **OK**.
   e. In the **Management Pack** list, select **Service Manager Incident Management Configuration Library**, and then click **OK**.
5. In the incident template form, follow these steps:
   a. In the **Support Group** box, select a tier. For example, if you want all printer-related

issues to be assigned to the tier 2 support group, select **Tier 2**.

b. Click **OK**.

c. Press F5 to refresh the **Templates** pane.

To validate that the new incident template was created

- Verify that the new incident templates are listed in the **Templates** pane.

Configuring Service Level Management in System Center 2012 - Service Manager

This section provides an overview of how to configure service level management in System Center 2012 – Service Manager. This section also contains procedures that cover service level management configuration scenarios.

Configuring Service Level Management Topics

- About Service Level Management

  Provides an overview of how to configure service level management.
- How to Create a Calendar Item

  Describes how to create a calendar item used by a service level objective.
- How to Edit a Calendar Item

  Describes how to edit a calendar item used by a service level objective.
- How to Create SLA Metrics

  Describes how to create a service level metric used by a service level objective.
- How to Edit SLA Metrics

  Describes how to edit a service level metric used by a service level objective.
- How to Modify an SLA Metric View

  Describes how to modify a SLA metric view to customize for your preference.
- How to Create a Service Level Objective

  Describes how to create a service level objective used by incidents and service requests to measure their timeliness.
- How to Edit a Service Level Objective

  Describes how to edit a service level objective used by incidents and service requests to measure their timeliness.
- How to View SLA Information in an Incident Form

  Describes how to view incident SLA information to determine whether the incidents are near breaching or have already breached.
- How to Review Incidents with SLA Information

Describes how to view incidents that have a service level objective associated with them.

- How to Send SLA Notification Information to the Assigned-To User

  Describes how to send periodic notifications to analysts responsible for incidents when each incident is within the warning period of its service level objective.

- How to Reactivate Incidents with SLA Information

  Describes how to reactivate resolved incidents that have an associated service level objective.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Service Level Management

Service level management is the process that you use to measure incident and service request timeliness. In System Center 2012 – Service Manager, you create a service level item that consist of queues that correspond to each service level, plus time metrics to measure and warn for. Separately, you can also send notifications to users that occur before and after service level breach. In the Service Manager console, you manage this process in the Administration workspace using the following nodes:

- Calendar
- Metric
- Service Level Objectives

Calendar

The Calendar node is used to define work days, work hours, and holidays as a calendar item in the Service Manager console. Each calendar item is a distinct work schedule that represents time available for analysts to resolve incidents and fulfill service requests. Calendar items correspond to at least one service level objective where it is measured by a time metric, such as resolution time.

Metric

The Metric node is used to define time metrics against a calendar item, corresponding to a service level objective. A time metric is the measurement between start and end dates. There are two predefined metrics inService Manager:

- Resolution Time
- Completion Time

The Resolution Time metric is used to measure the maximum length of time that incidents should take before they are resolved. By default, the two points in time that define Resolution Time are the start date as the date and time that each incident is created and the end date as the date and time that each incident is resolved.

The Completion Time metric is used to measure the maximum length of time that service requests should take before they are completed. By default, the two points in time that define Completion Time are the start date as the date and time that each service request is created and the end date as the date and time that each service request is completed.

Service Level Objectives

The Service Level Objectives node is used to create relationships between a queue and a service level. It is also used to define the relationship between a calendar item and a time metric. Separately, you can also send notifications to users that occur before and after service level breach. For more information about sending notifications, see How to Send SLA Notification Information to the Assigned-To User.

See Also

How to Send SLA Notification Information to the Assigned-To User

How to Create a Calendar Item

You create a calendar item to define work days, work hours, and holidays in System Center 2012 – Service Manager. After you create a calendar item, you will use it as part of a service level objective, where it is measured against a time metric.

To create a calendar item

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Calendar**.
3. In the **Tasks** pane, under **Calendar**, click **Create Calendar**.
4. In the **Create/Edit Calendar** dialog box, in the **Title** box, type a title for the calendar. For example, type **Normal Work Calendar**.
5. In the **Time zone** list, select the time zone of your location.
6. Under **Working days and hours**, select the work days of your organization and for each selected day, type the start and end time for each day.
7. Under **Holidays**, click **Add** to define any holidays that your organization does not normally work. In the **Add Holiday** dialog box, type the name and select the date of the holiday and then click **OK** to close the dialog box.
8. Click **OK** to close the **Create/Edit Calendar** dialog box.

How to Edit a Calendar Item

You edit a calendar item in System Center 2012 – Service Manager to update work days, work hours, and holidays. After you edit a calendar item, you will use it as part of a service level objective, where it is measured against a time metric. If the calendar is already associated with a service level objective, it appears in the **Related SLA(s)** area.

Note

When you update an existing calendar item, the update is effective for incidents and service requests created afterward; however, the updates do not affect existing incidents.

To edit a calendar item

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Calendar**.
3. In the Calendar list, select an existing calendar, and then in the **Tasks** pane, under **<CalendarName>**, click **Properties**.
4. In the **Create/Edit Calendar** dialog box, modify any of the following items, as needed:
   - **Title**
   - **Time zone**
   - **Working days and hours**
   - **Holidays**
5. Click **OK** to close the **Create/Edit Calendar** dialog box.

How to Create SLA Metrics

In System Center 2012 – Service Manager you create a service level management metric, which is analogous to service level agreements (SLAs), as a time metric to measure the difference between start and end times for incidents and service requests. After you define a metric, you associate it with a service level objective. If the metric is already associated with a service level objective, it appears in the **Related SLA(s)** area.

To create a metric for incidents

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Metric**.
3. In the **Create/Edit SLA Metric** dialog box, in the **Title** box, type a title for the metric. For example, type **Incident Metric**.
4. In the **Description** box, type a description of the metric. For example, type **Time that incidents are resolved**.
5. Under **Class**, click **Browse** to open the **Select a Class** dialog box, select **Incident**, and then click **OK** to close the dialog box.

6. Click the list next to **Start date** and then select the item that you want to use to define the start date. For example, select **First assigned date**.
7. Click the list next to **End date**, and then select the item that you want to use to define the end date. For example, select **Resolved date**.
8. Click **OK** to close the **Create/Edit SLA Metric** dialog box.

To create a metric for service requests

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Metric**.
3. In the **Create/Edit SLA Metric** dialog box, in the **Title** box, type a title for the metric. For example, type **Service Request Metric**.
4. In the **Description** box, type a description of the metric. For example, type **Time that service requests are completed**.
5. Under **Class**, click **Browse** to open the **Select a Class** dialog box, select **Service Request**, and then click **OK** to close the dialog box.
6. Click the list next to **Start date**, and then select the item that you want to use to define the start date. For example, select **First assigned date**.
7. Click the list next to **End date**, and then select the item that you want to use to define the end date. For example, select **Completed date**.
8. Click **OK** to close the **Create/Edit SLA Metric** dialog box.

How to Edit SLA Metrics

In System Center 2012 – Service Manager, you edit a service level agreement (SLA) metric to update the title, start date, and end date. After you edit a metric, you associate it with a service level objective. If the metric is already associated with a service level objective, it appears in the **Related SLA(s)** area.

Note

You should avoid making changes to an SLA metric that is in use because changing it might cause performance problems. If possible, edit in-use SLA metrics during a period of minimal system use, such during as a maintenance period.

To edit an SLA metric

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Metric**.
3. In the **Metric** list, select an existing metric, and then in the **Tasks** pane, under **<MetricName>**, click **Properties**.
4. In the **Create/Edit Metric** dialog box, modify any of the following items, as needed:
   - **Title**

- **Description**
- **Start date**
- **End date**

5. Click **OK** to close the **Create/Edit Metric** dialog box.

How to Modify an SLA Metric View

In System Center 2012 – Service Manager, you can use the following procedures to customize an SLA view.

Views let you group SLA metrics that share certain criteria. However, when you personalize changes to a view, those changes are not saved. For example, you can customize the **Metrics** view, but if you change column widths, column sorting, grouping, or if you remove columns, the next time you return to the view it displays information in the same manner as it did before you personalized it.

To personalize an SLA metric view

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then select **Metric**.
3. Right-click any view column heading to resize columns, to remove items from the results, or to change column sorting and grouping. Repeat this step until you are satisfied with the results.
4. You can also type in the **Filter** box to show results that are limited items that match what you typed.

How to Create a Service Level Objective

In System Center 2012 – Service Manager, you create a service level objective to create relationships between a queue and a service level, a calendar item and a time metric, and actions that occur before or after service level breaches. Afterward, when you view incidents or service requests and they approach their warning time, you will see a notification bar stating that the item is about to breach. You can also create periodic notifications if you want analysts to receive email for incidents or service requests that might breach their service level objective. For more information about sending notifications, see How to Send SLA Notification Information to the Assigned-To User.

In order to create a service level objective, it is easier if you have already created or defined a calendar item and an SLA metric. Additionally, the service level objective that you create is linked to a queue. The queue that you associate to a service level objective must target the same type of work item, based on its class; otherwise, the queue will not be available when you create the service level objective.

To create a service level objective

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Service Level Objective**.
3. In the **Tasks** pane, under **Service Level Objectives**, click **Create Service Level Objective**.
4. In the Create Service Level Objective Wizard, on the **Before You Begin** page, click **Next**.
5. On the **General** page, in the **Title** box, type a name for the new service level objective.
6. In the **Description** box, type a description of the service level objective.
7. Next to **Class**, click **Browse** to Open the **Select a Class** dialog box and then select a class pertinent to the type of service level objective you are creating. Normally, you should choose either **Incident** or **Service Request**.
8. Ensure that **Enabled** is selected, and then click **Next**.
9. On the **Service Level Criteria** page, select a calendar and a time metric, or you can create new ones. For more information about creating a calendar, see How to Edit a Calendar Item. For more information about creating an SLA metric, see How to Create SLA Metrics.
10. Under **Target**, specify the amount of time in hours or minutes that the work item should be completed by.
11. Under **Warning threshold**, specify the amount of time in hours or minutes before the service level is beached, which causes a warning notification in the work item notification bar, and then click **Next**.
12. On the **Summary** page confirm the choices you made, and then click **Create**.
13. On the **Completion** page, click **Close**.

See Also

How to Create a Calendar Item

How to Create SLA Metrics

How to Send SLA Notification Information to the Assigned-To User

How to Edit a Service Level Objective

In System Center 2012 – Service Manager, you can edit a service level objective to modify relationships between a queue and a service level, a calendar item and a time metric, and actions that occur before or after service level breaches. Afterward, when you view incidents or service requests and they approach their warning time, you will see a notification bar stating that the item is about to breach. You can also create periodic notifications if you want analysts to receive email for incidents or service requests that might breach their service level objective.

The service level objective that you edit is linked to a queue. If you want to modify the association of queue to a service level objective, the service level objective must target the same type of work item as the queue, based on its class; otherwise, the queue will not be available when you modify the service level objective.

To modify a service level objective

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Service Level Management**, and then click **Service Level Objective**.
3. In the **Service Level Objectives** list, select an existing service level objective, and then in the **Tasks** pane, under **<ServiceLevelObjectiveName>**, click **Properties**.
4. In the **Edit SLA** dialog box, modify any of the following items, as needed. For more information about the elements on this page, see How to Create a Service Level Objective.
   - **Title**
   - **Queues**
   - **Service Level Criteria**
5. Click **OK** to close the **Edit SLA** dialog box.

See Also

How to Create a Calendar Item

How to Create SLA Metrics

How to Create a Service Level Objective

How to View SLA Information in an Incident Form

As you are working with incidents in System Center 2012 – Service Manager, it is easy to tell when an incident's service level is about to or has been breached by viewing incidents in the **Assigned To Me** view and then looking for information in the **Service Level Target** column.

If you are already in an incident form and an incident is about to breach, a notification bar is displayed in the form while on the **General** tab stating that **One or more Service Level Objectives are about to breach.** You can view additional information about the service level status on the corresponding tab and see that the status shown is a warning.

When an incident has already been breached, no notification bar is displayed in the form while you are on the **General** tab. However, you will see breached status while you are on the **Service Level** tab if that incident's service level objective has breached.

To view warning SLA information in an incident form

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Incident Management**, and then click **Incidents with**

Service Level Warning.

3. In the **Incidents with Service Level Warning** list, select an incident, and then in the **Tasks** pane, under **<IncidentID-IncidentName>**, click **Edit**.
4. In the **<Incident IncidentID-IncidentName – Status>** form, observe the **One or more Service Level Objectives are about to breach** warning.
5. Click the **Service Level** tab, and observe the status of the incident as **Warning**. You can also see other information about the incident, most notably **Time Before SLA Breached**.
6. Click **OK** to close the incident.

To view breached SLA information in an incident form

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Incident Management**, and then click **Incidents with Service Level Breached**.
3. In the **Incidents with Service Level Breached** list, select an incident, and then in the **Tasks** pane, under **<IncidentID-IncidentName>**, click **Edit**.
4. Click the **Service Level** tab, and observe the status of the incident as **Breached**.
5. Click **OK** to close the incident.

How to Review Incidents with SLA Information

You can use the following procedure to view incidents that have a service level objective associated with them in System Center 2012 – Service Manager.

To review incidents with SLA information

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Incident Management**, and then click **Incidents with Service Level Warning** or **Incidents with Service Level Breached**.
3. In the list of incidents, notice the time that is displayed for **Service Level Target**.

How to Send SLA Notification Information to the Assigned-To User

In System Center 2012 – Service Manager, you can send notifications to analysts who are responsible for incidents when each incident is within the warning period of its service level objective. Because periodic notifications require a large amount of system resources, the following example notifies the analyst once when the service level objective goes to a warning state.

To send an SLA notification to the assigned-to user

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Notifications**, and then click **Subscriptions**.
3. In the **Tasks** pane, click **Create Subscription** to open the Create E-Mail Notification Subscription Wizard.
4. On the **Before You Begin** page, read the instructions, and then click **Next**.
5. On the **General** page, complete these steps:
   a. In the **Notification subscription name** box, type a name for the subscription for the service level objective.
   b. In the **Description** box, type a description of the subscription for the service level objective.
   c. In the **When to notify** list, select **When an object of the selected class is updated**.
   d. Next to **Targeted class** click **Browse** and then in then in the **Frequently used basic classes** list, select **All basic classes**. In the **Select a Class** dialog box, click **Service Level Instance Time Information**, and then click **OK** to close the dialog box.
   e. Keep the default management pack information, and then click **Next**.
6. On the **Group/Queue Selection** page, click **Next**.
7. On the **Additional Criteria** page, complete these steps:
   a. In the **Changed From** tab, set **[Service Level Instance Time Information] Status Does Not Equal Warning**.
   b. On the **Changed To** tab, set **[Service Level Instance Time Information] Status Equals Warning**, and then click **Next**.
8. On the **Template** page, select an email template or create a new one targeted at the Service Level Instance Time Information class. For more information about creating email notification templates, see How to Create Notification Templates. Click **Next**.
9. On the **Recipient** page, click **Add** and select the groups and users to send the notification to, and then click **Next**.
10. On the **Related Recipient** page, click **Add**, select **[WorkItem]WorkItem has Service Level Instance Information** in the left box, and then select **Primary Owner** and **Assigned To User** in the right box, and then click **Next**.
11. On the **Summary** page, review the information, and then click **Create**.
12. On the **Completion** page, click **OK** to close the wizard.

See Also

How to Create Notification Templates

How to Reactivate Incidents with SLA Information

In System Center 2012 – Service Manager, you can reactivate resolved incidents that have an associated service level objective. However, keep in mind that the original date and time that the incident was opened is preserved. Consequently, the time that elapsed while the incident was

resolved continues to apply against the service level objective—possibly resulting in the service level objective being breached.

To reactivate an incident with SLA information

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Incident Management**, and then click **All** .
3. In the **All Incidents** list, locate a resolved incident that you want to reactivate, and select it.
4. In the **Tasks** list, under **<IncidentID – IncidentTitle>**, click **Change Incident Status**, and then select **Activate**.
5. In the **Activate** box, type a comment describing why you are activating the incident, and then click **OK**.

Configuring Workflows in System Center 2012 - Service Manager

In System Center 2012 – Service Manager, a workflow is a sequence of activities that automate a business process. Workflows can, for example, update incidents when various changes occur. A workflow can automatically generate incidents when computers fall out of compliance from desired configuration management. You create a workflow that defines when and under what circumstances it will run. For example, a workflow can automatically change the support tier from a setting of 1 to 2 whenever a low-priority incident pertaining to printing problems is changed to a higher priority. Workflow activities function by the application of templates. For this example, an incident template to change the support tier to a setting of 2 must have been created previously.

You can create multiple workflows for each workflow configuration. You can enable or disable the workflow conditions. If a particular rule is disabled, the remaining rules still cause the workflow to run. If you want to completely disable a workflow, you must disable all of the rules that call the workflow.

The success or failure of a workflow is retained by Service Manager, and it is available for you to view. Two views are available. **All Results** consists of a view of all success and failure instances, and the **Errors** view displays only those instances when a workflow failed. In the **All Results** view, you can, for each instance, view the log and view the related object. When you view the log, you can examine the events that occurred when the workflow ran. When you view the related object, you see the form that this workflow acted on. The **Errors** view is limited to the most recent 250 instances. When you are viewing a failed instance, you have the same options in the **Success** view to view the log and view the related object. In addition, in the **Errors** view, you have the option to select **Retry** or **Ignore**. Selecting **Retry** causes the workflow to run again with the same parameters and removes this instance from the view. Selecting **Ignore** removes the instance from the view.

Configuring Workflow Topics

- How to Configure Incident Workflows

  Describes how to create an incident event workflow rule that changes the support tier level from 1 to 2 because of a change in incident priority.
- How to View Workflow Success or Failure

  Describes how to view the success or failure of a workflow.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Configure Incident Workflows

You can use the following procedure in System Center 2012 – Service Manager to create and configure a workflow rule that will change the support tier to **Tier 2** whenever the **Urgency** property of an incident that is related to printing problems is changed to **High**. This procedure assumes that you already created an incident template to change the support tier to **Tier 2**, and it assumes that you already created the priority calculation table. For more information, see How to Set Incident Priority and "To create a new printer-related incident template" in How to Create Incident Templates.

To configure an incident workflow

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Workflows**, and then click **Configuration**.
3. In the **Configuration** pane, double-click **Incident Event Workflow Configuration**.
4. In the **Configure Incident Event Workflows** dialog box, click **Add**.
5. In the **Add Incident Event Workflow** dialog box, complete these steps:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **Workflow Information** page, in the **Name** box, type a name for the workflow. For example, type **Escalates Printer Problems to Support Tier 2 when the Urgency property is changed to High**.
   c. In the **Check for events** list, select **when an object is created or when an object is updated**, make sure that the **Enabled** check box is selected, and then click **Next**.
   d. On the **Specify Event Criteria** page, click the **Changed to** tab. In the **Available Properties** list, select **Urgency**, and then click **Add**. In the **Criteria** box, select **equals**. In the list, select **High**. Then, click **Next**.
   e. On the **Select Incident Template** page, click **Apply the following template**, and then select the template you created earlier that will set the support group to **Tier 2**.

For example, select **Escalate Printer Problems to Tier 2**, and then click **Next**.

f. Optionally, in the **Select People to Notify** page, select the **Enable notification** check box, select the user to notify, and then click **Next**.

g. On the **Summary** page, review your settings, and then click **Create**.

h. On the **Completion** page, click **Close**.

6. In the **Configure Incident Event Workflows** dialog box, click **OK**.

To validate an incident workflow

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Work Items**, expand **Incident Management**, and then click **All Incidents**.
3. In the **All Incidents** pane, double-click an incident that is not currently assigned to the tier 2 support group.
4. In the **Incident Form** page, set the **Urgency** property to **High**, and then click **OK**.
5. In a few minutes, press F5. Verify that the value in the **Support Group** box changed to **Tier 2**.

You can use Windows PowerShell commands to complete these and other related tasks, as follows:

- For information about how to use Windows PowerShell to create a new workflow in Service Manager, see New-SCSMWorkflow.
- For information about how to use Windows PowerShell to retrieve configuration and status information for Service Manager workflows, see Get-SCSMWorkflowStatus.
- For information about how to use Windows PowerShell to update workflow properties, see Update-SCSMWorkflow cmdlet.
- For information about how to use Windows PowerShell to remove a workflow from Service Manager, see Remove-SCSMWorkflow.

How to View Workflow Success or Failure

Use the following procedure to view the success or failure instances of the workflows in System Center 2012 – Service Manager.

To view workflow success or failure

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Workflows**, and then click **Status**.
3. In the **Status** pane, click the workflow that you want to view. For example, click **Escalates Printer Problems to Support Tier 2 when the Urgency property is changed to High**.
4. In the **Status** results pane, click **Need attention** to view workflows that did not run

successfully. Or, click **All Instances**, and then do the following:

a. Click **View log** to view the list of events that occurred when the workflow ran.

b. Click **View related object** to view the form that was used when the workflow ran.

The status of each workflow is displayed in the **Status** column.

You can use a Windows PowerShell command to complete this task. For information about how to use Windows PowerShell to retrieve the status of workflows in Service Manager, see Get-SCSMWorkflowStatus.

Configuring Change and Activity Management in System Center 2012 - Service Manager

As part of your initial configuration of System Center 2012 – Service Manager, you have to configure settings and workflows for change and activity management. Create a change request template that you can use later when new change requests are submitted.

Configure workflows to automatically close completed change requests and send notifications to users when activities require approval. Workflows automate processes that you can use to automatically apply templates and send notifications.

A change request template is useful when you create a change request for a recurring type of issue because you can set an issue category and define a standard priority, effect, and risk level for it in the template. You can also create additional templates for other types of recurring change requests. Another benefit of creating a change request template is that users spend less time when they submit new change requests.

Configuring Change and Activity Management Topics

- How to Create Change Request Templates

  Describes how to construct a change request template to create change requests.
- How to Create a Manual Activity Template

  Describes how to create a manual activity template.
- How to Configure General Change Settings

  Describes how to configure settings that are used to specify a change request prefix and to define change request attachment limits.
- How to Configure General Activity Settings

  Describes how to configure settings that are used to specify prefixes for activities.
- How to Configure Change Management Workflows

  Describes how to configure change request conditions that can apply a change request template and send notifications.
- How to Configure Activity Management Workflows

Describes how to configure activity management conditions that can apply an activity template and send notifications.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Create Change Request Templates

Use the following procedures to create two change request templates in System Center 2012 – Service Manager and then validate them. The first template is used to create change requests to modify Microsoft Exchange Server infrastructure. The second template is used to automatically change the priority of a standard change request to **Low**. For more information about how to use the second template after you create it, see How to Configure Change Management Workflows.

Change request templates store commonly used settings and apply the information to new change requests. For example, you can create a change request template that includes a number of activities. However, activities that you want to include in a change request template must have been previously created as activity templates.

Note

When you create a change request template, do not create links to configuration items or work items, and do not enter any user information. If you create a template with these objects, you cannot remove them, and you will have to re-create the template.

To create a messaging change request template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, click **Templates**.
3. In the **Tasks** pane, under **Templates**, click **Create Template**.
4. In the **Create Template** dialog box, type a name for the template in the **Name** box. For example, type **Changes to Messaging Infrastructure Template**.
5. In the **Description** box, type a description for the template.

   For example, type **Use this change template when you want to modify the messaging infrastructure**.
6. Click **Browse** to select a class.
7. In the **Select a Class** dialog box, click **Change Request**, and then click **OK**.
8. In the **Create Template** dialog box, under **Management pack**, select **Service Manager Change Management Configuration Library**, and then click **OK**.
9. In the **Change Request Template** form, on the **General** tab, in the **Description** box, type a description for the change.

For example, type **Use when modifying the Exchange Server software infrastructure**.

10. In the **Area** box, select the area that is affected by the change request. For example, expand **Hardware**, and then select **Server**.
11. In the **Priority** box, select a value. For example, select **High**.
12. In the **Impact** box, select a value. For example, select **Standard**.
13. In the **Risk** box, select a value. For example, select **Medium**.
14. Click the **Activities** tab, and then click **Add**.
15. In the **Templates** list, select **Default Review Activity**, and then click **OK** to open the review activity form.
16. In the **Title** box, type a name for the review activity. For example, type **Messaging Infrastructure Request Approval**. Then, click **Add** to add the user or group that will normally approve the change request.
17. In each open form or dialog box, click **OK**.

To create a priority-modifying template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, click **Templates**.
3. In the **Tasks** pane, click **Create Template** under **Templates**.
4. In the **Create Template** dialog box, type a name for the template in the **Name** box. For example, type **Set Standard Change Requests to Low Priority**.
5. In the **Description** box, type a description for the template.

   For example, type **Use this change template to automatically set the priority for standard change requests to Low**.
6. Click **Browse** to add a class.
7. In the **Choose Class** dialog box, click **Change Request**, and then click **OK**.
8. In the **Create Template** dialog box, under **Management pack**, select **Service Manager Change Management Configuration Library**, and then click **OK**.
9. In the **Change Request Template** form, on the **General** tab, in the **Priority** list, select **Low**.
10. Click **OK**.

To validate template creation

- Verify that the new templates were created. For example, verify that **Changes to Messaging Infrastructure Template** and **Set Standard Change Requests to Low Priority** appear in the **Templates** view. You might have to press F5 to make the new change templates appear.

How to Create a Manual Activity Template

Use the following procedures to create a manual activity template in System Center 2012 – Service Manager and then validate it. Manual activity templates help ensure that all manual activities are assigned to the person who is the activity implementer. After you create the manual activity template, you create a workflow that applies the template. For more information about how to create a workflow, see How to Configure Incident Workflows.

In the following procedure, you will create a manual activity template named "Set <named user> as the Activity Implementer". This manual activity template is used in the How to Configure Activity Management Workflows procedure.

To create a manual activity template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, click **Templates**.
3. In the **Tasks** pane, in the **Templates** area, click **Create Template**.
4. In the **Create Template** dialog box, in the **Name** box, type a name for the template. For example, type **Set <named users> as the Activity Implementer**.
5. In the **Description** box, type a description for the template.
6. Click **Browse** to choose a class.
7. In the **Choose Class** dialog box, click **Manual Activity**, and then click **OK**.
8. In the **Create Template** dialog box, under **Management pack**, select **Service Manager Activity Management Configuration Library**, and then click **OK**.
9. In the **Manual Activity Template** form, on the **General** tab, click the ellipsis button (**…**) next to **Activity Implementer**, select a user, and then click **OK**.

To validate that the template was created

- In the **Templates** view, verify that the new template was created. You might have to press F5 to make the new manual activity template appear.

How to Configure General Change Settings

Use the following procedures in System Center 2012 – Service Manager to configure settings to specify change request prefixes and to define change request file attachment limits and then validate the settings.

Note
Revising the change request prefix does not affect existing change requests.

To configure general change settings

1. In the Service Manager console, click **Administration**.

2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Change Request Settings**.
4. In the **Tasks** pane, in the **Change Request Settings** area, click **Properties**.
5. In the **Change Request Settings** dialog box, you can make the following changes:
   a. If you want to change the prefix code, change the default value in the **Change Request ID prefix** box.
   b. If you want to change the maximum number of files that you can attach to a change request, change the default value in the **Maximum number of attached files** box. For example, type **2**.
   c. If you want to change the maximum size of files that you attach to a change request, change the default value in the **Maximum size (KB)** box. For example, type **300**.
6. Click **OK** to close the **Change Request Settings** dialog box.

To validate change settings

1. To validate changes to the prefix code, create a new a change request, and verify that the change request IDs have the prefix that you specified.
2. To validate changes to the attachment settings, open a change request, and attempt to add a file attachment that violates the settings that you specified.

How to Configure General Activity Settings

Use the following procedure in System Center 2012 – Service Manager to configure settings to specify activity prefixes when you view activity records. You can then validate the settings. You can define these activity settings in the administrative area of the Service Manager console.

Note
Revising the activity request prefix does not affect existing activity records.

To configure general activity settings

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** pane, click **Activity Settings**.
4. In the **Tasks** pane, in the **Activity Settings** area, click **Properties**.
5. In the **Activity Settings** dialog box, you can make the following changes:
   - If you want to change the activity prefix code, change the default value in the **Activity prefix** box. For example, change the value to **AA**.
   - If you want to change the manual activity prefix code, change the default value in the **Manual activity prefix** box. For example, change the value to **AM**.
   - If you want to change the review activity prefix code, change the default value in the **Review activity prefix** box. For example, change the value to **AR**.

6. Click **OK** to close the **Activity Settings** dialog box.

To validate activity setting changes

- To validate changes to any prefix code, create a new change request, and then verify on the **Activities** tab that the activities have the new prefix that you specified.

How to Configure Change Management Workflows

Use the following procedures in System Center 2012 – Service Manager to set the priority of all standard change requests and then validate the change. For example, you can set the priority of all standard change requests to low. In this procedure, you create a new workflow to automate the process.

Before you can complete the steps in this procedure, you have to create the following templates:

- **Set Standard Change Requests to Low Priority**: For more information, see the procedure "To create a priority-modifying template" in How to Create Change Request Templates.
- **New Standard Change Request Received Template**: For more information, see the procedure "To create a notification template for change requests" in How to Create Notification Templates.

To create a workflow to set all standard change requests to low

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Workflows**, and then click **Configuration**.
3. In the **Configuration** pane, click **Change Request Event Workflow Configuration**.
4. In the **Tasks** pane, in the **Change Request Event Workflow Configuration** area, click **Configure Workflow Rules**.
5. In the **Configure Workflows** dialog box, click **Add**.
6. On the **Before You Begin** page of the Configure Workflows for Objects of Class Change Request Wizard, click **Next**.
7. On the **Workflow Information** page, in the **Name** box, type a name for the workflow. For example, type **Set Standard Change Request to Low Priority workflow**.
8. Optionally, in the **Description** box, you can type a description of the new workflow. For example, you can type **This workflow automatically sets the priority of a standard change request to low**.
9. In the **Check for events** list, select **When an object is created**.
10. Make sure that the **Enabled** check box is selected, and then click **Next**.
11. On the **Specify Criteria** page, on the **Changed To** tab, in the **Related classes** list, select **Change Request**.
12. In the **Available properties** list, select **Category**, and then click **Add**. In the **Criteria** area, next to the **equals** box, select **Standard**, and then click **Next**.

13. On the **Apply Template** page, select the **Apply the selected template** check box.
14. In the **Templates** list, select **Set Standard Change Requests to Low Priority**, and then click **Next**.
15. On the **Select People to Notify** page, select the **Enable notification** check box.
16. Under **User**, select **Created By User**, and under **Template**, select **New Standard Change Request Received Template**, and then click **Add**.
17. Click **Next**.
18. On the **Summary** page, click **Create**.
19. On the **Completion** page, click **Close**.
20. In the **Configure Workflows** dialog box, click **OK**.

To validate workflow creation

1. In the **Configuration** pane, select the **Change Request Event Workflow Configuration** template.
2. In the **Tasks** pane, click **Configure Workflow Rules**.
3. In the **Configure Workflows** dialog box, the **Set Standard Change Request to Low Priority workflow** workflow should appear.
4. Optionally, you can create a new change request by using the **Standard Change Request** template to verify that the priority of new requests is set to Low.
5. Notification email is sent to the user who created the change request.

How to Configure Activity Management Workflows

Use the following procedures in System Center 2012 – Service Manager to automatically assign all unassigned manual activities to a named user and then validate the creation of workflow.

Before you can complete the steps in this procedure, you have to create the following templates:

- **Set <named user> as the Activity Implementer**: For more information, see How to Create a Manual Activity Template.
- **New Activity Assigned Received Template**: For more information, see How to Create Notification Templates.

The new workflow you are about to create applies the **Set <named user> as the Activity Implementer** template, which assigns the named user all the activities that do not have a designated activity implementer. The **New Activity Assigned Received Template** sends notification to a user if the email notification channel is configured.

To create an activity management workflow

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Workflows**, and then click **Configuration**.

3. In the **Configuration** pane, click **Activity Event Workflow Configuration**.
4. In the **Tasks** pane, in the **Activity Event Workflow Configuration** area, click **Configure Workflow Rules**.
5. In the **Select a Class** dialog box, in the **Name** list, select **Manual Activity**, and then click **OK**.
6. In the **Configure Workflows** dialog box, click **Add**.
7. On the **Before You Begin** page of the **Configure workflows for objects of class Manual Activity** wizard, click **Next**.
8. On the **Workflow Information** page, in the **Name** box, type a name for the workflow. For example, type **Assign Unassigned Activities to <named user>**.
9. Optionally, in the **Description** box, you can type a description of the new workflow. For example, you can type **This workflow automatically assigns unassigned manual activities to the <named user>**.
10. In the **Check for events** list, select **When an object is created**.
11. Make sure that the **Enabled** check box is selected, and then click **Next**.
12. On the **Specify Criteria** page, on the **Changed to** tab, in the **Related classes** list, select **Manual Activity**.
13. In the **Available properties** list, select the **Stage** check box, and then click **Add**.
14. In the **Criteria** area, next to the **[Activity] Stage** box, select **equals**, select **Approve** for the value, and then click **Next**.
15. On the **Apply Template** page, make sure that **Apply the selected template** check box is selected.
16. In the **Templates** list, select **Set <named users> as the Activity Implementer**, and then click **Next**.
17. On the **Select People to Notify** page, select the **Enable notification** check box.
18. In the **User** list, select **Assigned to User**.
19. In the **Message template** list, select **New Activity Assigned Received Template**, click **Add**, and then click **Next**.
20. On the **Summary** page, click **Create**.
21. On the **Completion** page, click **Close**.
22. In the **Configure Workflows** dialog box, click **OK** to close it.

To validate workflow creation

1. In the **Administration** pane, expand **Administration**, expand **Workflows**, and then click **Status**.
2. In the **Status** pane, verify that the new workflow template titled **Assign Unassigned Activities to the <named user>** is listed.

Configuring Release Management in System Center 2012 - Service Manager

As part of your initial configuration of System Center 2012 – Service Manager, you have to configure settings and workflows for release management. The settings define the ID prefix that is assigned to release records, how many files can be attached to each release record, and the maximum size of each file. You also create a workflow to notify people when a release record affects them.

Configuring Release Management Topics

- How to Configure Release Management Settings

  Describes how to configure settings for release management.
- How to Configure Release Management Workflows for Notifications

  Describes how to configure release management workflows for notifications.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Configure Release Management Settings

The System Center 2012 – Service Manager Administrator configures release management settings by using the following procedure.

Note

Revising the release record prefix does not affect existing release records.

To configure release management settings

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, and then click **Settings**.
3. In the **Settings** view, click **Release Management Settings**.
4. In the **Tasks** pane, in the **Release Management Settings** area, click **Properties**.
5. In the **Release Management Settings** dialog box, you can make the following changes:
   a. If you want to change the prefix code, change the default value in the **Release Record ID prefix** box.
   b. If you want to change the maximum number of files that you can attach to a release record, change the default value in the **Maximum number of attached files** box. For example, type **2**.

c. If you want to change the maximum size of files that you attach to a release record, change the default value in the **Maximum size (KB)** box. For example, type **300**.

6. Click **OK** to close the **Release Management Settings** dialog box.

How to Configure Release Management Workflows for Notifications

You can configure notifications for release records in System Center 2012 – Service Manager by completing the following procedures. The following procedure sends a notification when a release record is created or updated.

To configure a notification for updated release records

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Workflows**, and then click **Configuration**.
3. In the **Configuration** pane, double-click **Release Record Event Workflow Configuration**.
4. In the **Configure Workflows** dialog box, click **Add**.
5. In the **Configure workflows for objects of class Release Record** dialog box, complete these steps:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **Workflow Information** page, in the **Name** box, type a name for the workflow. For example, type **Updated Release Records**.
   c. In the **Description** box, type a description of what the workflow does. For example, type **This workflow notifies the assigned-to user and the created-by user when release records are updated.**
   d. In the **Check for events** list, select **When an object is created** or select **When an object is updated**, ensure that the **Enabled** check box is selected, and then click **Next**.
   e. On the **Specify Event Criteria** page, click the **Changed to** tab. Under **Related classes**, expand **Release Record**, and then select either **Assigned To User** or **Created By User**.
   f. Under **Available properties**, select **User Name**, click **Add**, and then under **Criteria**, type the user name of the person that you are basing the notification on. Repeat this step, as necessary.
   g. On the **Apply Template** page, clear **Apply the selected template**, and then click **Next**.
   h. On the **Select People to Notify** page, select **Enable notification**, then select **Assigned To User** and then click **Add**. Repeat this step for **Created By User**, and then click **Next**.
   i. On the **Summary** page, review your settings, and then click **Create**.

j. On the **Completion** page, click **Close**.

Configuring Desired Configuration Management to Generate Incidents in System Center 2012 - Service Manager

You can use the following procedure, for example, to inventory all the computers that might require an upgrade to Microsoft Exchange Server with Service Pack 1 (SP1). To do this, first define the appropriate configuration baseline in System Center Configuration Manager 2007. For more information about baselines in Configuration Manager 2007, see How to Configure Configuration Baselines for Desired Configuration Management.

In System Center 2012 – Service Manager, you must create a Configuration Manager connector to import the baseline and configure incident management to automatically generate incidents based on desired configuration management. For information about how to create a Configuration Manager connector, see About Importing Data from System Center Configuration Manager.

You can use desired configuration management in Configuration Manager 2007 to monitor software to ensure that it is compliant with defined values. For example, you can monitor software versions, security settings, and software updates. The configurations that you want to monitor are added as Configuration Manager 2007 configuration items to configuration baselines so that they can be evaluated for compliance as a group.

In Service Manager, you can import configuration baselines from Configuration Manager 2007 by using a Configuration Manager Connector. You can then configure Service Manager to create incidents for each Service Manager configuration item that reports as noncompliant against the defined values.

Use the following procedure to configure incident management to automatically generate incidents based on desired configuration management.

Configuring Desired Configuration Management Topics

- How to Configure Desired Configuration Management to Generate Incidents

  Describes how to configure incident management to automatically generate incidents based on desired configuration management.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Configure Desired Configuration Management to Generate Incidents

In System Center 2012 – Service Manager, you can import configuration baselines from System Center Configuration Manager 2007 by using a Configuration Manager connector. Then, you can configure Service Manager to create incidents for each Service Manager configuration item that is reported as noncompliant against the defined values.

You can use the following procedures to configure incident management to automatically generate desired configuration management–based incidents and validate that the desired configuration management is configured.

To configure incident management to automatically generate desired configuration management–based incidents

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Workflows**, and then click **Configuration**.
3. In the **Configuration** pane, double-click **Desired Configuration Management Event Workflow Configuration**.
4. In the **Configure Desired Configuration Management Workflows** dialog box, click **Add**.
5. In the Add Desired Configuration Management Workflow Wizard, complete these steps:
   a. On the **Before You Begin** page, click **Next**.

      Note
      The **Next** button will be unavailable if a Configuration Manager connector has not been created.

   b. On the **Workflow Information** page, type a name and a description for the rule. Make sure that the **Enabled** check box is selected, and then click **Next**.
   c. On the **Select System Center Configuration Manager Configuration Items** page, expand all the configuration baselines that are listed, select the Configuration Manager 2007 configuration items that you want to include in the rule, and then click **Next**.
   d. On the **Select Incident Template** page, click **Apply the following template**, select a template for the new incidents that will be created by this rule, and then click **Next**.
   e. On the **Select People to Notify** page, select the **Enable notification** check box. Select the users who should be notified when an incident is created by this rule. For each user, specify the notification method and a template, and then click **Add**. Click **Next**.
   f. On the **Summary** page, make sure that the settings contain the information you expect, and then click **Create**.
   g. On the **Completion** page, make sure that you receive the following confirmation message, and then click **Close**:

      “Desired Configuration Management Workflow Created Successfully”

To validate that desired configuration management is configured

1. Import an out-of-compliance Service Manager configuration item that would match one of the desired configuration management rules. Then, locate the desired configuration management–based incident in Service Manager.
2. In the Service Manager console, click **Work Items**
3. In the **Work Items** pane, expand **Incident Management**, and then click **All Open DCM Incidents**.
4. In the **All Open Desired Configuration Management Incidents** pane, double-click an incident.
5. In the **Incident** form, click the **Compliance Errors** tab.
6. Verify that the correct configuration baseline and Configuration Manager 2007 configuration items are listed.

You can use Windows PowerShell commands to complete these and other related tasks, as follows:

- For information about how to use Windows PowerShell to create a desired configuration management workflow in Service Manager, see New-SCSMDCMWorkflow.
- For information about how to use Windows PowerShell to retrieve the list of all DCM workflows that are defined in Service Manager, see Get-SCSMDCMWorkflow.
- For information about how to use Windows PowerShell to update properties of a desired configuration management workflow, see Update-SCSMDCMWorkflow.
- For information about how to use Windows PowerShell to remove a desired configuration management workflow from Service Manager, see Remove-SCSMDCMWorkflow.

Configuring System Center 2012 - Service Manager Notifications

You may want to be notified by email when incidents or other changes in System Center 2012 – Service Manager. By using Service Manager, you can make sure that notifications are generated for almost any kind of change. For example, you can configure notifications to be sent to a messaging analyst when changes occur to a work item or configuration item that pertains to email problems.

Before notifications are sent, first configure each notification channel, such as the settings for Simple Mail Transfer Protocol (SMTP). Notification messages are sent based on a notification template. Therefore, you must create a notification template. You can then use the Notification Subscription Wizard to subscribe a group of users to a notification that will be sent whenever the changes that you specify occur. Finally, you can verify that a notification is sent by manually generating the change.

You must complete these steps in the order shown. For example, before you can configure a notification, the SMTP channel must be enabled.

Note

You must add the Service Manager workflow account to the Service Manager Administrators user role for notifications to function properly. See the topic "How to Add a Member to a User Role" in the Administrator's Guide for System Center 2012 - Service Manager.

Configuring Notifications Topics

- How to Configure Notification Channels

  Describes how to set up a notification channel.
- How to Create Notification Templates

  Describes how to set up a notification template.
- How to Subscribe to Notifications

  Describes how to subscribe to a notification for yourself or for others.
- How to Verify a Notification Configuration

  Describes how to verify that notification configuration is set up correctly.
- About Substitution Strings in Notification Templates

  Describes how you can use substitution strings to insert information into notification templates.
- How to Automatically Notify Groups of Users

  Describes how to create a messaging-enabled group and a workflow to notify stakeholders when an incident is created.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Configure Notification Channels

You can use the following procedures to configure notification channels in System Center 2012 – Service Manager and validate the configuration. Notification channels are the method by which notification messages are sent to users. You use the **Configure E-Mail Notification Channel** dialog box to configure and enable email notifications that Service Manager sends to a Simple Mail Transfer Protocol (SMTP) server.

Note

In this release of Service Manager, only email notification is supported.

To configure email notifications

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Notifications**, and then click **Channels**.
3. In the **Channels** pane, click **E-Mail Notification Channel**.
4. In the **Tasks** pane, under **E-Mail Notification Channel**, click **Properties** to open the **Configure E-Mail Notification Channel** dialog box.
5. Select the **Enable e-mail notifications** check box.
6. Click **Add**. In the **Add SMTP Server** dialog box, type the fully qualified domain name (FQDN) of the SMTP server that you want to use. For example, type **Exchange01.Woodgrove.Com**.
7. In the **Port number** box, type or select the SMTP port number that you want to use. For example, select **25**.
8. In the **Authentication method** box, select either **Anonymous** or **Windows Integrated**. For example, select **Anonymous**. Then, click **OK**.
9. In the **Return e-mail address** box, type the email address of the service account that is used during setup. For example, type **smadmin@woodgrove.com**.
10. In the **Retry primary after** box, type or select the number of seconds that you want Service Manager to wait before it tries to resend outgoing email notifications. For example, select **25**.
11. Click **OK** to close the dialog box.

To validate email notification configuration

1. In the **Channels** pane, click **E-Mail Notification Channel**.
2. In the **Tasks** pane, under **E-Mail Notification Channel**, click **Properties** to open the **Configure E-Mail Notification Channel** dialog box.
3. Verify that the configuration you entered is correct.

You can use a Windows PowerShell command to complete these tasks, as follows:

- For information about how to use Windows PowerShell to set the properties of an email notification channel in Service Manager, see Set-SCSMChannel.
- For information about how to use Windows PowerShell to retrieve the Email Notification channels that are defined in Service Manager, see Get-SCSMChannel.

How to Create Notification Templates

You can use the following procedures in System Center 2012 – Service Manager to create notification templates for many types of information records or work items that Service Manager records or keeps track of, such as incidents, change requests, activities, release records, and configuration items. After you create the notification templates, you can use a notification subscription to send email messages based on the templates. The notification template determines the type and format of the messages to send.

Note

Manually copying and pasting substitution strings from other notification templates will not generally work. Therefore, you should avoid copying them to prevent errors. Instead, you can easily browse for and insert available substitution strings into any notification template that you are creating or updating. For more information about using substitution strings in notification templates, see About Substitution Strings in Notification Templates.

The following two templates are prerequisites for other procedures:

- The New Activity Assigned Received Template, which is described in the procedure "To create a notification template for a newly assigned activity," is the template that you will need for the procedure **How to Configure Activity Management Workflows**.
- The New Standard Change Request Received Template, which is described in the procedure "To create a notification template for change requests," is the template that you will need for the procedure **How to Configure Change Management Workflows**.

Note

In this release of Service Manager, notifications are sent only by email.

To create a notification template for incidents

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Notifications**, and then click **Templates**.
3. In the **Tasks** pane, under **Templates**, click **Create E-mail Template**.
4. On the **General** page of the Create E-mail Notification Template Wizard, in the **Notification template name** box, type a name. For example, type **New E-mail Incident Template**. Optionally, in the **Description** box, you can type a description for the template that you are creating.
5. Next to the **Targeted class** box, click **Browse**.
6. In the **Choose Class** dialog box, click **Incident**, and then click **OK**.
7. Make sure that an unsealed management pack of your choice is selected, and then click **Next**. For example, select the **Sample Management Pack**.
8. On the **Template Design** page, in the **Message subject** box, type a subject for the email template. For example, type **New Incident created with ID#**. Then, click **Insert**.
9. In the **Select Property** dialog box, select **ID**, and then click **Add**.
10. In the **Message body** box, type a description to indicate that a new incident was opened for an email problem.
11. Use the other default values on this page, and then click **Next**.
12. On the **Summary** page, review the settings that you have selected for the template. Then, click **Create**.
13. On the **Completion** page, click **Close**.

To create a notification template for change requests

1. In the Service Manager console, click **Administration**.

2. In the **Administration** pane, expand **Notifications**, and then click **Templates**.
3. In the **Tasks** pane, under **Templates**, click **Create E-mail Template**.
4. On the **General** page of the Create E-mail Notification Template Wizard, in the **Notification template name** box, type a name. For example, type **New Standard Change Request Received Template**. Optionally, in the **Description** box, you can type a description for the template that you are creating.
5. Next to the **Targeted class** box, click **Browse**.
6. In the **Choose Class** dialog box, click **Change Request**, and then click **OK**.
7. Make sure that an unsealed management pack of your choice is selected, and then click **Next**. For example, select the **Sample Management Pack**.
8. On the **Template Design** page, in the **Message subject** box, type a subject for the email template. For example, type **New Standard Change Request with ID#**. Then, click **Insert**.
9. In the **Select Property** dialog box, select **ID**, and then click **Add**.
10. In the **Message body** box, type a description to indicate that a new standard change request was opened.
11. Use the other default values on this page, and then click **Next**.
12. On the **Summary** page, review the settings that you have selected for the template. Then, click **Create**.
13. On the **Completion** page, click **Close**.

To create a notification template for a newly assigned activity

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Notifications**, and then click **Templates**.
3. In the **Tasks** pane, under **Templates**, click **Create E-mail Template**.
4. On the **General** page of the Create E-mail Notification Template Wizard, in the **Notification template name** box, type a name. For example, type **New Activity Assigned Received Template**. Optionally, in the **Description** box, you can type a description for the template that you are creating.
5. Next to the **Targeted class** box, click **Browse**.
6. In the **Select a Class** dialog box, click **Manual Activity**, and then click **OK**.
7. Make sure that an unsealed management pack of your choice is selected, and then click **Next**. For example, select the **Sample Management Pack**.
8. On the **Template Design** page, in the **Message subject** box, type a subject for the email template. For example, type **New Activity Assigned with ID#**. Then, click **Insert**.
9. In the **Select Property** dialog box, select **ID**, and then click **Add**.
10. In the **Message body** box, type a description to indicate that an activity has been assigned.
11. Use the other default values on this page, and then click **Next**.
12. On the **Summary** page, review the settings that you have selected for the template. Then, click **Create**.

13. On the **Completion** page, click **Close**.

To validate template creation

- Verify that the new template you created appears in the list of notification templates.

You can use Windows PowerShell commands to complete these and other related tasks, as follows:

- For information about how to use Windows PowerShell to create a new Email template in Service Manager, see New-SCSMEmailTemplate.
- For information about how to use Windows PowerShell to retrieve Email templates that are defined in Service Manager, see Get-SCSMEmailTemplate.
- For information about how to use Windows PowerShell to retrieve the content of a Service Manager Email template, see Get-SCSMEmailTemplateContent.
- For information about how to use Windows PowerShell to update properties of an Email template, see Update-SCSMEmailtemplate.
- For information about how to use Windows PowerShell to remove an Email template from Service Manager, see Remove-SCSMEmailTemplate.

See Also

About Substitution Strings in Notification Templates

How to Subscribe to Notifications

After you create a notification template, and after you have enabled at least one notification channel, you can use the following procedure in System Center 2012 – Service Manager to subscribe to notifications by using the Notification Subscription Wizard. Then, notifications will be sent when an object is created or updated or periodically when other criteria that you specify are met.

The scenarios in this topic center on the Create E-Mail Notification Subscription Wizard. The condition that you choose to notify will dynamically change the wizard pages that are available.

In the first procedure, you set up a subscription so that a messaging analyst is notified when a new incident that pertains to an email problem is opened. In the second procedure, you set up a subscription so that daily status updates are sent to the release manager while the HR web application is in development, testing, and deployment.

Note

Some notification criteria values might not change. If you want to receive a notification when a change occurs, make sure that you choose a value for an object that is likely to change. For example, the **Incident ID** for an incident does not change.

To create a notification subscription for an incident

1. In the Service Manager console, click **Administration**.

2. In the **Administration** pane, expand **Notification**, and then click **Subscriptions**.
3. In the **Tasks** pane, click **Create Subscription**.
4. On the **Before You Begin** page of the Create E-mail Notification Subscription Wizard, click **Next**.
5. On the **General** page, in the **Notification subscription name** box, type a name. For example, type **New Incident for E-mail Problem Notification Subscription**. Optionally, in the **Description** box, you can type a description for the subscription that you are creating.
6. Next to the **Targeted class** box, click **Browse**.
7. In the **When to notify** box, select **When an object of the selected class is created**.
8. In the **Choose Class** dialog box, choose a class. For example, click **Incident**. Then, click **OK**.
9. Make sure that an unsealed management pack of your choice is selected, and then click **Next**. For example, select the **Sample Management Pack**.
10. On the **Additional Criteria** page, select **Incident**. In the **Available Properties** list, select **Classification Category**, and then click **Add**.
11. On the **Additional Criteria** page, click the **Criteria** tab. In the **Criteria** area, next to **[Incident] Classification Category**, select **equals**. In the list, select **E-mail Problems**, and then click **Next**.
12. On the **Template** page, next to the **E-mail template** box, click **Select**.
13. In the **Select Objects** dialog box, in the **Templates** list, select a notification template. For example, select **New E-mail Incident Template**, click **OK**, and then click **Next**.
14. On the **Recipient** page, click **Add**.
15. In the **Select Objects** dialog box, search for the appropriate user, and then select the user. Click **Add**, click **OK**, and then click **Next**. For example, select the user account for a messaging analyst or messaging administrator.

    Note
    The notification address must be configured for the user account of the messaging analyst or messaging administrator.
16. On the **Related Recipients** page, click **Add**.
17. In the **Select Related Recipient** dialog box, search for the appropriate class, and then select the appropriate substitution string that represents the user. Click **Add**, click **OK**, and then click **Next**. For example, select additional user accounts that you want to send the notification to.
18. On the **Summary** page, review the settings that you selected for the notification subscription, and then click **Create**.
19. On the **Completion** page, click **Close**.

To create a periodic notification subscription for a release record

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Notifications**, and then click **Subscriptions**.

3. In the **Tasks** pane, click **Create Subscription**.
4. On the **Before You Begin** page of the Create E-mail Notification Subscription Wizard, click **Next**.
5. On the **General** page, in the **Notification subscription name** box, type a name. For example, type **Daily Notification for Deploy HR Web 2.0 Release Record**. Optionally, in the **Description** box, you can type a description for the subscription that you are creating. For example, type **This subscription sends a daily notification of the status for the HR Web 2.0 release record**.
6. In the **When to notify** box, select **Periodically notify when objects meet a criteria**.
7. Next to the **Targeted class** box, click **Browse**.
8. In the **Choose Class** dialog box, choose a class, and then click **OK**. For example, click **Release Record**.
9. Make sure that an unsealed management pack of your choice is selected, and then click **Next**. For example, select the **Sample Management Pack**.
10. On the **Additional Criteria** page, select **Release Record**. In the **Available Properties** list, select **Status**, and then click **Add**.
11. In the **Criteria** area, next to **[Release Record] Status**, select **does not equal**. In the list, select **Closed**, and then click **Next**.
12. On the **Recurring Notification** page under **Recurrence pattern**, select **Notify every <TimeInterval>** and then choose an interval. For example, set the recurrence pattern to every 1 day.
13. On the **Recurring Notification** page under **Range of recurrence**, select a range of recurrence or choose no end date. For example, select **No end date**.
14. On the **Template** page, next to the **E-mail template** box, click **Select**.
15. In the **Select Template** dialog box, in the **Templates** list, select a notification template that you have created for release record notifications.
16. On the **Recipient** page, click **Add**.
17. In the **Select Objects** dialog box, search for the appropriate user, and then select the user. Click **Add**, click **OK**, and then click **Next**. For example, select the user account for the release manager.

    Note
    The notification address must be configured for the user account of the messaging analyst or messaging administrator.
18. On the **Related Recipients** page, click **Add**.
19. In the **Select Related Recipient** dialog box, search for the appropriate class, and then select the appropriate substitution string that represents the user. Click **Add**, click **OK**, and then click **Next**. For example, select additional user accounts that you want to send the notification to.
20. On the **Summary** page, review the settings that you selected for the notification subscription, and then click **Create**.
21. On the **Completion** page, click **Close**.

To validate a notification subscription

- Locate the notification subscription that you created in the list of subscriptions.

You can use a Windows PowerShell command to complete these tasks and other related tasks, as follows:

- For information about how to use Windows PowerShell to create a new subscription in Service Manager, see New-SCSMSubscription.
- For information about how to use Windows PowerShell to retrieve subscriptions that are configured in Service Manager, see Get-SCSMSubscription.
- For information about how to use Windows PowerShell to update subscription properties in Service Manager, see Update-SCSMSubscription.
- For information about how to use Windows PowerShell to remove a subscription from Service Manager, see Remove-SCSMSubscription.

See Also

How to Configure Notification Channels

How to Create Notification Templates

How to Verify a Notification Configuration

You can use the following procedure in System Center 2012 – Service Manager to verify that you have correctly configured notifications. Generate the type of change that activates the notification subscription that was previously created. When you do this, the subscription generates and then sends a notification. Receipt of the notification verifies success. For example, create a test incident that generates an email notification. The notification informs the recipient that an incident was opened.

If you are verifying a recurring notification subscription, you must wait for the time interval that you set previously to elapse until the notification is sent. When the notification is received, the configuration of the notification is verified.

To verify a notification configuration

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Work Items**, expand **Incident Management**, and then click **All Open Incidents**.
3. In the **Tasks** pane, under **Incident Management**, click **Create Incident**.
4. In the **Incident <Number> New** form, enter the required information in the **Affected user**, **Title**, **Classification Category**, **Impact**, and **Urgency** boxes.
5. In the **Classification Category** list, select **E-mail Problems**, and then click **OK**.
6. Verify that an email notification that contains the information you entered in the template is received. The email title should contain the incident ID number.

About Substitution Strings in Notification Templates

Substitution strings are special tokens or system variables that are used in notification templates in System Center 2012 – Service Manager. These strings retrieve properties from an instance that is related to the instance for which the template was created. The strings then display the value in the notification email. Notification templates in Service Manager include substitution strings. Although you should avoid modifying the predefined templates, you can duplicate them and then modify the duplicates.

For example, the end user notification template includes a substitution string in the message body that represents the user's first name. If you want to add the user's last name, you can easily do so by using the **Insert** button, which is available when you edit a notification template, and then browsing the available strings that are available for the class of template that you are modifying. In this example, you would browse and then select **Affected User** and then select **Last Name** to insert the string into the template. Later, when the notification is sent to the user, his or her first and last name is included in the message as a salutation.

While this example is very simple, Service Manager includes substitution strings for almost every property that you might need to create notifications that can inform end users and other Service Manager users with very timely and relevant information. You can easily view the substitution strings that are available in Service Manager by opening an existing notification template and then, in the template design area, clicking the **Insert** button to view the classes and properties.

See Also

How to Create Notification Templates

How to Automatically Notify Groups of Users

In some scenarios, you may want to use a group rather than an individual user in System Center 2012 – Service Manager as a work item stakeholder. For example, you might want to assign an incident to a team of people, such as an initial response team that routes incidents, and then notify everyone in the initial response team that an incident has been assigned to their team.

Messaging-enabled universal security groups in Microsoft Exchange Server are the key to this task. Although you can create these groups in Exchange Server 2007, this topic describes how to accomplish this using the Exchange Server 2010 Exchange Management console for incidents. You can use the following procedures to create a messaging-enabled universal security group, create a workflow to notify stakeholders when an incident is created, and then test for success.

In Exchange Server 2007 and later versions, the **Require that all senders are authenticated** setting is enabled by default for mail-enabled universal security groups. You can modify the setting in the distribution group properties, in Mail-Flow settings, in the **Message Delivery Restrictions** dialog box. If your outgoing Simple Mail Transfer Protocol (SMTP) server specified in the Service Manager settings (Under **Administration**>**Notifications Channels**>**Edit**) is using

Anonymous as the Authentication Method (either in Service Manager or the SMTP settings), then given the above default setting in exchange, the email would not be sent out. If you have Anonymous Access configured on the SMTP side, it is necessary either to clear the **Require that all senders are authenticated** setting in exchange for the Mail Enabled Universal Security Group, or change the SMTP authentication settings (in Service Manager or the outgoing SMTP Server settings) from anonymous to Windows Integrated, so that the user is authenticated, allowing the email to be sent.

As an alternative, you can avoid using **Assigned to** and instead use **Support Group** changing as a triggering field. To set this up, create a new email notification subscription, and under additional criteria, use the following:

- Changed from: [incident] Support Group Does not equal Tier 1
- Changed to: [incident] Support Group equals Tier 1

Use whatever template you want, and add the recipient of the mailing distribution list for Tier 1. Now Tier 1 is notified whenever a ticket is set to them, even if it is done by means of a template at portal ticket creation.

Setting up one of these for each support group will ensure that all your groups are informed of incoming incidents that require their attention.

To create a messaging-enabled universal security group

1. In the Exchange Management Console, navigate to **Recipient Configuration**, right-click **Distribution Group**, and then click **New Distribution Group**.
2. On the **Introduction** page, either choose an existing universal group or create a new group.
3. On the **Group Information** page, select the **Security** group type.
4. Complete the creation of the group.
5. Add members to the group by right-clicking them, clicking **Properties**, and accessing the **Members** tab.
6. Wait for Service Manager to sync with Active Directory Domain Services (AD DS), or perform a manual Synchronization from **Administration**>**Connectors**. (Click **AD Connector**, and then click the **Synchronize Now** task on the right-hand side).
7. Once the Active Directory synchronization has completed, the newly created group will be available as a configuration item in Service Manager, and it can be selected in the user picker fields, such as **Affected User** and **Assigned To**.

To create a workflow to notify stakeholders when an incident is created

1. Navigate to **Administration**>**Workflows**>**Configuration**.
2. Double-click **Incident Event Workflow Configuration**.
3. Click **Add**, and then click **Next** on the **Before you Begin** page.
4. Give the workflow a name, such as “Incident Created – Email Stakeholders”.
5. Leave the default of **When an incident is created** in the **Check for Events** drop-down

list.

6. Select one of your custom management packs (or create one) to store the workflow in, and then click **Next**.
7. Click **Next** on the **Specify Incident Criteria** page. (We want this workflow to run when any new incident is created.)
8. Optionally, apply a template. (In this case we are creating the workflow for notification only, so we choose **Do not apply a template**.)
9. In the **Select People to Notify** dialog box, select the **Enable notification** check box. Add the appropriate users you want to notify with the appropriate templates.
10. Click Next, and then click **Create** to complete creation of the workflow.

To test the workflow and mail the enabled universal security group

1. Create an incident and assign it to the messaging-enabled universal security group that you created earlier.

See Also

Automatically Notifying Groups of Users

Using the Service Catalog in System Center 2012 - Service Manager

This section provides an overview of how to use the service catalog in System Center 2012 – Service Manager. This section also contains procedures that cover management configuration scenarios for the service catalog.

Service Catalog Topics

- About the Service Catalog

  Provides an overview of how to configure and manage the service catalog.
- How to Extend the Service Offering Categories

  Describes how to add additional categories of service offerings to the service catalog.
- How to Create a Service Offering

  Describes how to create a service offering.
- How to Create Service Request Templates for New Request Offerings

  Describes how to create offering templates that are used to create new request offerings.
- How to Create a Request Offering

  Describes how to create a new request offering.
- How to Publish a Request Offering

  Describes how to publish a request offering.
- How to Unpublish a Request Offering

Describes how to unpublish a request offering.

- How to Add Request Offerings to Service Offerings

  Describes how to add request offerings to service offerings.
- How to Create a Catalog Item Group

  Describes how to create a catalog item group and associate the group to a user role and queue.
- How to Specify a User Role for Catalog Items

  Describes how to create a user role and associate it to a catalog group a set of users.
- How to Copy Request Offerings and Service Offerings

  Describes how to copy request offerings and service offerings.
- How to Publish a Service Offering

  Describes how to publish a service offering.
- How to Create and Categorize Catalog Items in Localized Languages

  Describes how to create and categorize catalog items in localized languages.
- How to Edit a Service Offering or a Request Offering

  Describes how to edit a service offering or a request offering.
- How to Delete a Service Offering or a Request Offering

  Describes how to delete a service offering or a request offering.
- About Languages Supported by the Service Catalog

  Explains how localized languages are supported by the service catalog.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About the Service Catalog

The service catalog is a collection of items, assistance, actions, or groupings of them that your IT staff and infrastructure provides and makes available to end users in the Self-Service Portal in System Center 2012 – Service Manager. In the Service Manager console, you create catalog items to describe these items in the Library workspace using the following nodes:

- Request Offerings
- Service Offerings

The Request Offerings node is used to create a catalog item that describes an item, assistance, or action that is available to end users. It also defines information that you want to prompt the users for and any knowledge articles that are associated with the offering.

After it is created, you can set the status of a request offering as either Draft or Published. Draft status indicates that a request offering is not published and available to the service catalog. This prevents end users from requesting the offering. When you set the request offering status to Published, it appears in the catalog where users can request it, if they have been granted access to a catalog item group that contains the request offering. It is possible to create a request offering that is not part of a service offering. In this case, the request offering appears in the Self-Service Portal under an uncategorized list view.

The Service Offerings node is used to create a catalog item that categorizes request offerings.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Extend the Service Offering Categories

By default, System Center 2012 – Service Manager includes only the General service offering category. However, your organization will likely need additional categories to help organize service offerings that are provided to end users through the service catalog. You can use the following procedure to add additional categories to the service catalog.

To extend the service offering categories

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, click **Lists**, and then in the **Filter** box, type **offering**.
3. In the **Lists** view, select **Service Offering Category**, and then in the **Tasks** list under **Service Offering Category**, click **Properties**.
4. In the **List Properties** dialog box, add any service offering categories that you want, and then click **OK** to close the dialog box. For example, add the following categories:
   - **Data Center**
   - **Access and Security**
   - **Communication Services**
5. Click **OK** to close the **List Properties** dialog box.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Create a Service Offering

Service offerings are logical groups of request offerings in System Center 2012 – Service Manager. Both service offerings and their request offerings are available to Self-Service Portal users, when their status is set to Published and if end users have been assigned a corresponding Service Manager user role. Only users who have been assigned a user role that is

associated with a catalog group that contains catalog items can use the Self-Service Portal to access the service catalog.

To create a service offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Service Offerings**.
3. In the **Tasks** pane under **Service Offerings**, click **Create Service Offering** to open the Create Service Offering Wizard.
4. On the **Before You Begin** page, read the instructions, and then click **Next**.
5. On the **General** page, complete these steps:
   a. In the **Title** box, type a title for the service offering. For example, type **Access Services**.
   b. Optionally, next to **Image**, you can either **Browse** to an image file or leave the default selection.
   c. In the **Category** list, select a category that this service offering will be a part of. For example, select **Access and Security**.
   d. In the **Language** list, either leave the default selection or select a language.
   e. In the **Overview** text box, type a short overview to describe the service offering that will be shown on the Self-Service Portal home page. For example, type **Access to AD Group, Access to Labs**.
   f. In the description box, type a description that will appear on the service offering page in the Self-Service Portal.
   g. Next to **Management pack**, select an unsealed management pack of your choice, and then click **Next**. For example, if you previously created the Sample Management Pack, select it.
6. On the **Detailed Information** page, complete these steps:
   a. In the **Service level agreement information** box, type a summary of the service level agreement (SLA) information. For example, type **The SLAs for these requests, depending on the criticality of the requests, range from 1-2 business days. For more information, click the link below.**
   b. In the first **Link for additional information** box, type a hyperlink that users can click to view additional information about the SLA for this service offering.
   c. In the **Cost information** box, type a summary of any costs associated with requests that will be grouped in this service offering.
   d. In the second **Link for additional information** box, type a hyperlink that users can click to view additional information about any costs associated with requests that will be grouped in this service offering.
   e. Click **Next**.
7. Optionally, on the **Related Services** page, add related business services associated with the service offering, and then click **Next**.
8. Optionally, on the **Knowledge Articles** page, add related knowledge articles associated

with the service offering, and then click **Next**.

9. Optionally, on the **Request Offering** page, add related request offerings associated with the service offering, and then click **Next**.
10. On **the Publish** page, in the **Offering status** list, select **Published** and set the **Offering owner** to yourself, and then click **Next**.
11. On the **Summary** page, review the information, and then click **Create**.
12. On the **Completion** page, click **Close**.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Create Service Request Templates for New Request Offerings

By default, System Center 2012 – Service Manager includes a number of service request templates that are based on a generic incident template. By viewing the template, you can gain an understanding of the categories of information to collect and convey to end users as they submit requests through the Self-Service Portal. You can use the following procedure to create a new service request template without using the default generic incident request template.

To create a service request template

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, click **Templates**, and then in the **Tasks** lists under **Templates**, click **Create Template**.
3. In the **Create Template** dialog box, in the **Name** box, type a name for the template. For example, type **Request Membership to Group**.
4. In the **Description** box, type a description for the template. For example, type **This template is used to request membership to a group**.
5. Next to **Class**, click **Browse**, select **Service Request**, and then click **OK**.
6. Click **OK** to close the **Create Template** dialog box and open the **Service Request Template** form in template mode.
7. In the **Service Request Template** form, in the **Title** box, type **Request membership to Active Directory group**.
8. In the **Description** box, type a description of the purpose of the form. For example, type **This template is used to request membership to an Active Directory group**.
9. In the **Urgency** list, select **Medium**, and in the **Priority** list, select **Medium**.
10. In the **Source** list, select **Portal**, and then click the **Activities** tab.
11. On the **Activities** tab, click the **Add** button to open the **Select Template** dialog box, where you will add an activity.
12. Select **Default Review Activity**, and then click **OK** to close the **Select Template** dialog box and open the **Review Activity Template** dialog box.

13. In the **Title** box, type a name for the review activity. For example, type **Approval for the user Requesting Membership to AD Group**.
14. Click **Add** to open the **Reviewer** dialog box and select a user who will approve requests for this service request, and then click **OK** to close the dialog box.
15. Click **OK** to close the **Review Activity Template** form.
16. Add another activity, and then select the **Default Manual Activity** template.
17. In the **Manual Activity Template** form, in the **Title** box, type a title for the manual activity. For example, type **Add the requesting user to list of Active Directory groups in the impacted configuration items**.
18. Next to **Activity Implementer**, select a user who is responsible for the activity, and then click **OK** to close the **Manual Activity Template** form.
19. Click **OK** to close the **Service Request Template** form.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Create a Request Offering

Request offerings are catalog items that describe the item, assistance, or action that is available to end users in the service catalog in System Center 2012 – Service Manager. Request offerings are normally placed in logical groups of service offerings. Both service offerings and their request offerings are available to Self-Service Portal users when the status of the offerings is set to Published and if end users have been assigned a corresponding Service Manager user role. Only users who have been assigned a user role associated with a catalog group that contains catalog items can use the Self-Service Portal to access the service catalog.

You can use the following procedure to create a request offering.

To create a request offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Request Offerings**.
3. In the **Tasks** pane under **Request Offerings**, click **Create Request Offering** to open the Create Request Offering Wizard.
4. On the **Before You Begin** page, read the instructions, and then click **Next**.
5. On the **General** page, complete these steps:
   a. In the **Title** box, type a title for the request offering. For example, type **Access to Active Directory group**.
   b. Optionally, next to **Image**, you can either **Browse** to an image file, or leave the default selection.
   c. In the **Description** text box, type a short description that describes the request offering that will appear on the Self-Service Portal page. For example, type **Use this request offering to request membership to an Active Directory Group**.

d. Under **Select template**, select **Service Request**, and then in the **Select Template** dialog box, select a template that you created previously for a service request. For example, select the **Request Membership to Group** template, and then click **OK**.

e. Next to **Management pack**, select an unsealed management pack of your choice, and then click **Next**. For example, if you previously created the Sample Management Pack, select it.

6. On the **User Prompts** page, enter questions for users or define other instructions which will appear in the Self-Service Portal when a user submits a request by completing the following steps:

   a. In the **Form instructions** box, type a summary of the information that the user must provide for the request. For example, type **Provide the information below to request membership to the Active Directory Group**

   b. Under **Enter prompts or information text**, click **Add**; in the **User Prompts or Information** box, type **Enter your cost center**; in the **Response Type** list, select **Required**; and in the **Prompt Type** list, select **Integer**.

   c. In the second **Enter Prompts or Information** box, type **Select the list of Active Directory groups that you need access to**; in the **Response Type** list, select **Required**; and in the **Prompt Type** list, select **Query Results**.

   d. In the third **Enter Prompts or Information** box, type **Enter your justification for this request**; in the **Response Type** list, select **Required**; and in the **Prompt Type** list, select **Text**.

   e. Click **Next**.

7. On the **Configure Prompts** page, configure prompts to constrain user input to ensure that users provide the information required to fulfill their requests by completing the following steps:

   a. Select the **Enter your cost center** prompt, and then click **Configure**.

   b. In the **Configure Integer Control** dialog box, select **Limit integer range**, set the **Minimum Value** to **1000** set the **Maximum Value** to **6999**, and then click **OK** to close the dialog box.

   c. Select the **Select the Active Directory groups that you want access to** prompt, and click **Configure** to open the **Configure Instance Picker** dialog box.

   d. In the **Configure Instance Picker** dialog box in the **Frequently used basic classes** list, select **All basic classes**; in the filter box, type **Active**; and then select **Active Directory Group**.

   e. Click the **Configure Criteria (optional)** tab; in the list of properties under **User**, select **Department**; and then click **Add Constraint**.

   f. In the **Criteria** box, select **Department equals**; in the **Set Token** list, click **Select token**; and then click **1. Enter your cost center: Integer**.

   g. If the condition is not set to **equals**, select **equals**.

   h. Click the **Display Columns** tab, and then select **Display Name**, **Department**, and **Last Name**.

   i. Click the **Options** tab, select **Allow the user to select multiple objects**, and then select **Add user-selected objects as affected configuration items**.

j. Click **Ok** to close the **Configure Instance Picker** dialog box, and then click **Next**.

8. On the **Map Prompts** page, associate prompts with various fields of a service request or its activities, depending on the complexity of the form and the extension of the class that you have made. Complete the following steps to associate the justification to the review activity:

   k. .a. Select **Approval for the user requesting membership to the Active Directory group – (Review Activity)**.

   b. Next to **Description**, select the box under **Prompt Output**, and then in the list, select **3. Enter your justification: String**.

   c. Click **Next**.

9. Optionally, on the **Knowledge Articles** page you can select a knowledge article to associate with this request offering, and then click **Next**.
10. Optionally, on the **Publish** page, you can set publishing information, and then click **Next**.
11. On the **Summary** page, review the information, and then click **Create**.
12. On the **Completion** page, click **Close**.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Publish a Request Offering

You can publish draft request offerings in System Center 2012 – Service Manager by using the Publish task or by using a change request. When you publish a request offering by using the Publish task, no additional interaction is required, and the request offering appears in the Self-Service Portal as an uncategorized item. If you want to publish the request offering as part of a category, you must add the request offering to a service offering.

If you want to have an approval process added before publishing, you can associate the request offering to a change request. If you use a change request, you can also send email notifications as the approval process occurs.

Note

Various errors might occur if you create a request offering without mapped prompts or if you have erroneously mapped any prompts. The errors can occur after you associate a change request to the request offering and then you complete the change request. To avoid such errors, ensure that you have least one prompt in the request offering and that all prompts are mapped correctly.

You can use the following procedures to publish request offerings.

To publish draft request offerings

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Draft Request Offerings**.

3. In the **Draft Request Offerings** list, select one or more request offerings, and in the **Tasks** pane under **<RequestOfferingName>**, click **Publish**.

To use a change request to publish draft request offerings

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Draft Request Offerings**.
3. In the **Draft Request Offerings** list, select one or more request offerings, and in the **Tasks** pane under **<RequestOfferingName>**, click **Create Change Request to Publish**.
4. In the **Select Template** dialog box, select the **Publish Offering** change request template, and then click **OK** to open a new change request form.
5. In the **<ChangeRequestID: Publish Offerings>** form, notice that the catalog items to publish appear under **Catalog items**.
6. Click the **Activities** tab, and notice that there is a review activity and an automated activity associated with the change request. Later, when the review activity is approved, the automated activity will set the publish status to Published.
7. Click **OK** to save the change request.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Unpublish a Request Offering

When you unpublish a request offering in System Center 2012 – Service Manager, it is removed from the Self-Service Portal so that end users cannot request it. You can use the following procedure to unpublish a request offering.

To unpublish a request offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Published Request Offerings**.
3. In the **Published Request Offerings** list, select one or more request offerings, and in the **Tasks** pane under **<RequestOfferingName>**, click **Unpublish**.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Add Request Offerings to Service Offerings

In System Center 2012 – Service Manager, service offerings are logical groups of request offerings. For a service offering to appear in the Self-Service Portal, each service offering must

have at least one request offering added to it. After a service offering and a request offering are published, it is a straightforward process to associate them as a collection.

To add request offerings to service offerings

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Published Request Offerings**.
3. In the **Published Request Offerings** list, select one or more request offerings, and in the **Tasks** pane under **<RequestOfferingName>**, click **Add to Service Offering**.
4. In the **Select objects** dialog box, select the service offering that you want to associate the request offering with, click **Add**, and then click **OK** to close the dialog box.

How to Create a Catalog Item Group

Catalog item groups in System Center 2012 – Service Manager are lists of catalog items that are used to secure the service catalog and provide access to users, based on membership in a corresponding Service Manager user role. In the following procedure, you create a simple catalog item group. After you create the group, use an existing user role, or create a new user role, to provide access to catalog items that have been associated with the group.

To create a catalog item group

1. In the Service Manager console, select **Library**, and then click **Groups**.
2. In the **Tasks** pane under **Groups**, click **Create Catalog Group** to open the Create Group Wizard.
3. On the **Before You Begin** page, read the instructions, and then click **Next**.
4. On the **General** page, complete these steps:
   a. In the **Group name** box, type a name for the catalog group. For example, type **Access Request Offering Group**.
   b. In the **Group description** box, type a description for the catalog group. For example, type **This group is used to consolidate and provide security to Access Request Offering catalog items**.
   c. Next to **Management pack**, select an unsealed management pack of your choice, and then click **Next**. For example, if you previously created the Sample Management Pack, select it.
5. On the **Included Members** page, complete these steps to select catalog items and associate them with the catalog group:
   a. Click **Add** to open the **Select objects** dialog box, select one or more catalog items that you created previously, click **Add**, and then click **OK** to close the dialog box.
   b. Click **Next**.
6. Optionally, on the **Dynamic Members** page, you can select a class and specific objects,

based on the criteria that you choose, to add as members of the group, and then click **Next**.

7. Optionally, on the **Subgroups** page, you can add other groups as members of the new group that you are creating, and then click **Next**.
8. Optionally, on the **Excluded Members** page, you can select a class and specific objects, based on criteria that you choose, to exclude as members of the group, and then click **Next**.
9. On the **Summary** page, review the information, and then click **Create**.
10. On the **Completion** page, click **Close**.

See Also

Using the Service Catalog in System Center 2012 - Service Manager

How to Specify a User Role for Catalog Items

User roles in System Center 2012 – Service Manager provide access to catalog groups that contain catalog items. Both service offerings and their request offerings are available to Self-Service Portal users, when the status of the offerings is set to Published and if end users have been assigned a corresponding Service Manager user role. Only users who have been assigned a user role associated with a catalog group that contains catalog items can use the Self-Service Portal to access the service catalog. You can use the following procedure to create a user role and associate catalog items and users with the role.

To create a user role and associate it with catalog items and users

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Security**, and then select **User Roles**.
3. In the **Tasks** pane under **User Roles**, click **Create User Role**, and then click **End User** to open the Create User Role Wizard.
4. On the **Before You Begin** page, read the instructions, and then click **Next**.
5. On the **General** page, complete these steps:
   a. In the **Name** box, type a name for the user role. For example, type **Security Offerings End User Role**.
   b. Optionally, in the **Description** box, type a description of the purpose of the user role. For example, type **This user role provides access to security offerings to end users**.
   c. Click **Next**.
6. On the **Management Packs** page, complete these steps:
   a. In **Management Packs** list, select a management pack that is used by catalog items. For example, select **Service Manager Service Request Configuration Library**.
   b. Click **Next**.
7. On the **Queues** page, there are no options that apply to security to catalog items;

therefore, click **Next**.

8. On the **Configuration Item Groups** page, there are no options that apply to security to catalog items; therefore, click **Next**.
9. On the **Catalog Item Groups** page, select **Provide access to only the selected groups**, select the groups that you want to provide access to, and then click **Next**.
10. On the **Form Templates** page, ensure that **All forms can be accessed** is selected, and then click **Next**.
11. On the **Users** page, add the users and groups that you want to provide access to, and then click **Next**.
12. On the **Summary** page, review the information, and then click **Create**.
13. On the **Completion** page, click **Close**.

How to Copy Request Offerings and Service Offerings

After you create a request offering or a service offering in System Center 2012 – Service Manager, you can copy the offering so that you can easily modify the copied offering.

You can use the following procedures to copy a request offering and a service offering. Keep in mind that if you copy a published catalog item, the published status of the copy is set to Draft.

To copy a request offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, expand **Request Offerings**, and then select **All Request Offerings**.
3. In the **All Request Offerings** list, select the request offering that you want to copy, and then in the **Tasks** pane under **<RequestOfferingName>**, click **Create a Copy** to open the **Copy Request Offering** dialog box.
4. In the dialog box, you can optionally select **Also create a copy of the template referred to in this Request Offering** to create a copy of the template.
5. Optionally, you can change the management pack where information about the copied request offering is stored or you can create a new management pack.
6. Click **OK** to close the dialog box and create the copy.
7. The copied item appears in the list, with a prefix of **Copy of**. For example, your copy might have the name **Copy of Access to Active Directory Group**.

To copy a service offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, expand **Service Offerings**, and then select **All Service Offerings**.
3. In the **All Service Offerings** list, select the service offering that you want to copy, and then in the **Tasks** pane under **<ServiceOfferingName>**, click **Create a Copy** to open the

Copy Service Offering dialog box.

4. Optionally, you can change the management pack where information about the copied service offering is stored or you can create a new management pack.
5. Click **OK** to close the dialog box and create the copy.
6. The copied item appears in the list, with a prefix of **Copy of**. For example, your copy might have the name **Copy of Access Services**.

How to Publish a Service Offering

You can publish draft service offerings in System Center 2012 – Service Manager by using the Publish task or by using a change request. When you publish a service offering by using the Publish task, the service offing must contain at least one published request offering before it appears in the Self-Service Portal. If you want to have an approval process added before publishing, you can associate the service offering with a change request. If you use a change request, you can also send email notifications as the approval process occurs.

You can use the following procedures to publish a draft service offering and then use a change request to publish it.

To publish a draft service offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Draft Service Offerings**.
3. In the **Draft Service Offerings** list, select one or more service offerings, and in the **Tasks** pane under **<ServiceOfferingName>**, click **Publish**.

To use a change request to publish a draft service offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, and then select **Draft Service Offerings**.
3. In the **Draft Service Offerings** list, select one or more service offerings, and in the **Tasks** pane under **<ServiceOfferingName>**, click **Create Change Request to Publish**.
4. In the **Select Template** dialog box, select the **Publish Offering** change request template, and then click **OK** to open a new change request form.
5. In the **<ChangeRequestID: Publish Offerings>** form, notice that the catalog items to be published appear under **Catalog items**.
6. Click the **Activities** tab, and notice that there is a review activity and an automated activity associated with the change request. Later, when the review activity is approved, the automated activity will set the publish status to Published.
7. Click **OK** to save the change request.

How to Create and Categorize Catalog Items in Localized Languages

In System Center 2012 – Service Manager, you create and categorize catalog items for localized languages in the same manner that you do for U.S. English. The only difference is that when you create a service offering and a request offering, you do it in the localized language. By doing so, you can create catalog items in the language that is used by the end user who will submit requests. Service Manager includes catalog items that have been localized in various languages so that you can copy them and then modify them for use in your organization.

After you have created the service offering and request offerings in a localized language, users need to have the appropriate SharePoint language pack installed on the computers they use to view the Self-Service Portal. Additionally, they must select the appropriate language in the Self-Service Portal using **Site Settings** in **Site Administration** and then the appropriate selection of the default and alternate language they want to use with **Language Settings**.

To create and categorize catalog items in a localized language

1. Perform any necessary procedures in the topic How to Copy Request Offerings and Service Offerings to copy catalog items that have been localized.
2. Perform any necessary procedures in the topic How to Create a Service Offering, and ensure that you select the language of the catalog item.
3. Perform any necessary procedures in the topic How to Create Service Request Templates for New Request Offerings.
4. Perform any necessary procedures in the topic How to Create a Request Offering.
5. Perform any necessary procedures in the topic How to Add Request Offerings to Service Offerings.
6. Perform any necessary procedures in the topic How to Create a Catalog Item Group.
7. Perform any necessary procedures in the topic How to Specify a User Role for Catalog Items.
8. Perform any necessary procedures in the topics How to Publish a Request Offering and How to Publish a Service Offering.

See Also

About Languages Supported by the Service Catalog

How to Edit a Service Offering or a Request Offering

In System Center 2012 – Service Manager, request offerings are catalog items that describe the item, assistance, or action that is available to end users in the service catalog. Request offerings are normally placed in logical groups of service offerings. Both service offerings and their request offerings are available to Self-Service Portal users, when the status of the offerings is set to Published and if end users have been assigned a corresponding Service Manager user role. Only

users that have been assigned a user role that is associated with a catalog group that contains catalog items can use the Self-Service Portal to access the service catalog.

You can use the following procedures to edit a service offering or a request offering.

To edit a request offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, expand **Request Offerings**, and then select **All Request Offerings**.
3. In the **All Request Offerings** list, double-click the request offering that you want to edit.
4. In the **Edit Request Offering** form, you can edit information on the following pages:
5. On the **General** page, complete these steps:
   a. In the **Title** box, type a title for the request offering. For example, type **Access to Active Directory group**.
   b. Optionally, next to **Image**, you can either click **Browse** to find an image file or leave the default selection.
   c. In the **Description** text box, type a short description that will describe the request offering that will appear on the Self-Service Portal page. For example, type **Use this request offering to request membership to an Active Directory Group**.
6. On the **User Prompts** page, enter questions for users or define other instructions that will appear on the Self-Service Portal when a user submits a request by completing the following steps:
   a. In the **Form instructions** box, type a summary of the information that the user must provide for the request. For example, type **Provide the information below to request membership to the Active Directory Group**
   b. Under **Enter prompts or information text**, click **Add**; in the **User Prompts or Information** box, type **Enter your cost center**; in the **Response Type** list, select **Required**; and in the **Prompt Type** list, select **Integer**.
   c. In the second **Enter Prompts or Information** box, type **Select the list of Active Directory groups that you need access to**; in the **Response Type** list, select **Required**; and in the **Prompt Type** list, select **Query Results**.
   d. In the third **Enter Prompts or Information** box, type **Enter your justification for this request**; in the **Response Type** list, select **Required**; and in the **Prompt Type** list, select **Text**.
7. On the **Configure Prompts** page, configure prompts to constrain user input to ensure that users provide the information necessary to fulfill their request by completing the following steps:
   a. Select the **Enter your cost center** prompt, and then click **Configure**.
   b. In the **Configure Integer Control** dialog box, select **Limit integer range**, set the **Minimum Value** to **1000**, set the **Maximum Value** to **6999**, and then click **OK** to close the dialog box.
   c. Select the **Select the Active Directory groups that you want access to** prompt, and click **Configure** to open the **Configure Instance Picker** dialog box.

d. In the **Configure Instance Picker** dialog box in the **Frequently user basic classes** list, select **All basic classes**; in the filter box, type **Active**; and then select **Active Directory Group**.

e. Click the **Configure Criteria (optional)** tab; in the list of properties under **User**, select **Department**; and then click **Add Constraint**.

f. In the **Criteria** box, click **Department equals**; in the **Set Token** list, click **Select token**; and then click **1. Enter your cost center: Integer**.

g. If the condition is not set to **equals**, select **equals**.

h. Click the **Display Columns** tab, and then select **Display Name**, **Department**, and **Last Name**.

i. Click the **Options** tab, select **Allow the user to select multiple objects**, select **Add user-selected objects as affected configuration items**, and then select **Add the requesting user to the list of Active Directory group in the impacted configuration items (Manual Activity)**.

j. Click **Ok** to close the **Configure Instance Picker** dialog box.

8. On the **Map Prompts** page, associate prompts with various fields of a service request or its activities, depending on the complexity of the form and the extension of the class that you have made. Complete the following steps to associate a justification with the review activity:

   a. Select **Approval for the user requesting membership to the Active Directory group – (Review Activity)**.

   b. Next to **Description**, select the box under **Prompt Output**, and then in the list, select **3. Enter your justification: String**.

9. Optionally, on the **Knowledge Articles** page, you can select a knowledge article to associate with this request offering.

10. Optionally, on the **Publish** page, you can set publishing information.

11. Click **OK** to close the **Edit Request Offering** form.

To edit a service offering

1. In the Service Manager console, select **Library**.

2. In the **Library** pane, expand **Service Catalog**, expand **Service Offerings**, and then select **All Service Offerings**.

3. In the **All Service Offerings** list, double-click the service offering that you want to edit.

4. In the **Edit Service Offering** form, edit information on the following pages.

5. On the **General** page, complete these steps:

   a. In the **Title** box, type a title for the service offering. For example, type **Access Services**.

   b. Optionally, next to **Image**, you can either click **Browse** to find an image file, or leave the default selection.

   c. In the **Category** list, select a category that will be the group for this service offering. For example, select **Access and Security**.

d. In the **Language** list, either leave the default selection or select a language.

e. In the **Overview** text box, type a short overview that will describe the service offering that will appear on the Self-Service Portal home page. For example, type **Access to AD Group, Access to Labs**.

f. In the description box, type a description that will appear on the service offering page on the Self-Service Portal.

6. On the **Detailed Information** page, complete these steps:

   a. In the **Service level agreement information** box, type a summary of the service level agreement (SLA) information. For example, type **The SLAs for these requests range from 1-2 business days. For more information, click the link below.**

   b. In the first **Link for additional information** box, type a hyperlink that users can click to view additional information about the SLA for this service offering.

   c. In the **Cost information** box, type a summary of any costs associated with requests that will be grouped in this service offering.

   d. In the second **Link for additional information** box, type a hyperlink that users can click to view additional information about any costs associated with requests that will be grouped in this service offering.

7. Optionally, on the **Related Services** page, add related business services associated with the service offering.
8. Optionally, on the **Knowledge Articles** page, add related knowledge articles associated with the service offering.
9. Optionally, on the **Request Offering** page, add related request offerings associated with the service offering.
10. On the **Publish** page in the **Offering status** list, select **Published**, and then set the **Offering owner** to yourself.
11. Click **OK** to close the **Edit Service Offering** form.

How to Delete a Service Offering or a Request Offering

In System Center 2012 – Service Manager, service offerings and their request offerings are available to Self-Service Portal users, when the status of the offering is set to Published and if end users have been assigned a corresponding Service Manager user role. Only users who have been assigned a user role associated with a catalog group that contains catalog items can use the Self-Service Portal to access the service catalog. You can also delete a catalog item when it is no longer needed.

You can use the following procedures to delete a service offering or a request offering.

To delete a service offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, expand **Service Offerings**, and then select **All Service Offerings**.

3. In the **All Service Offerings** list, select the service offering that you want to delete.
4. In the **Tasks** list under **<ServiceOfferingName>**, click **Delete**.
5. In the **Delete Item** dialog box, click **Yes**.

To delete a request offering

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, expand **Service Catalog**, expand **Request Offerings**, and then select **All Request Offerings**.
3. In the **All Request Offerings** list, select the request offering that you want to delete.
4. In the **Tasks** list under **<RequestOfferingName>**, click **Delete**.
5. In the **Delete Item** dialog box, click **Yes**.

About Languages Supported by the Service Catalog

The Self-Service Portal in System Center 2012 – Service Manager supports many localized languages for service offerings. The following is a list of languages that are supported in Microsoft SharePoint 2010 products and in Service Manager. These languages are supported in the Service Manager console by means of the service offering **Language** item that you select. Accordingly, after you install the appropriate SharePoint 2010 language pack on the server that hosts SharePoint 2010 and the Self-Service Portal, you can select the corresponding SharePoint Language ID in the Self-Service Portal by using **Site Settings** in **Site Administration** and then selecting the default and alternate languages that you want to use with **Language Settings**.

Note

There is an exception for East Asian languages. Specifically, in the Service Manager console you must select **Chinese (Traditional, Taiwan)** and **Chinese (Simplified)** instead of the **Chinese (Traditional)** and **Chinese (Simplified, China)** options that the Self-Service Portal and SharePoint 2010 display.

The Service Manager console supports more languages than the languages in the following table. You can use languages—that are available in the Self-Service Portal and not listed in the table—in Silverlight modules when you localize the modules in other languages and then host them outside SharePoint 2010.

Supported SharePoint Foundation 2010 and SharePoint Server 2010 Languages

SharePoint 2010 Language	SharePoint 2010 Language ID
Arabic	1025
Basque (Basque)	1069

SharePoint 2010 Language	SharePoint 2010 Language ID
Bulgarian	1026
Catalan	1027
Chinese (Simplified)	2052
Chinese (Traditional)	1028
Croatian	1050
Czech	1029
Danish	1030
Dutch	1043
English	1033
Estonian	1061
Finnish	1035
French	1036
Galician	1110
German	1031
Greek	1032
Hebrew	1037
Hindi	1081
Hungarian	1038
Italian	1040
Japanese	1041
Kazakh	1087
Korean	1042
Latvian	1062
Lithuanian	1063
Norwegian (Bokmål)	1044
Polish	1045
Portuguese (Brazil)	1046
Portuguese (Portugal)	2070

SharePoint 2010 Language	SharePoint 2010 Language ID
Romanian	1048
Russian	1049
Serbian (Latin)	2074
Slovak	1051
Slovenian	1060
Spanish	3082
Swedish	1053
Thai	1054
Turkish	1055
Ukrainian	1058

Using Groups, Queues, and Lists in System Center 2012 - Service Manager

In System Center 2012 – Service Manager, you can use groups to manage configuration items, queues to manage work items, and lists to customize forms to classify different objects, such as incidents, change requests, activities, or configuration items. Use the overview and the procedures in the following topics to help manage these items.

Groups, Queues, and Lists Topics

- About Groups, Queues, and Lists

  Provides an overview of groups, queues, and lists in Service Manager.
- How to Create a Group

  Describes how to create a group.
- How to Create a Queue

  Describes how to create a queue.
- How to Edit a Queue

  Describes how to edit a queue.
- How to Add a List Item

  Describes how to add a list item.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager

- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Groups, Queues, and Lists

The **Library** pane in System Center 2012 – Service Manager contains items, such as groups, queues, and lists. You can use groups to manage configuration items, and you can use queues to manage work items. You can use lists to customize forms.

Using Groups to Manage Configuration Items

In Service Manager, groups contain objects. Typically, these objects are configuration items. Groups can include collections of objects of the same class or of different classes. For example, say that you decide to create the **Exchange Servers** group. You have several methods to do this. You can create a static group, a dynamic group, or a combination of static and dynamic groups. A static group is defined by specific objects, such as "Exchange1" and "Exchange2". A dynamic group is defined by inclusion rules. Inclusion rules are based on comparing a formula to the actual property value of a configuration item. The following table shows samples of inclusion rules.

Class.Property	Operator	Value
Active Directory.Domain	Contains	Woodgrove
Windows Server.Display Name	Contains	Exchange Servers
Operating System.Display Name	Starts with	Windows Server

For example, say that you want to restrict access to Exchange servers to only specific users. To do this, you create a new group that is named **Exchange Servers** and add all Exchange servers in this environment to the group. Later, you can configure user roles to limit access to the **Exchange Servers** group to only the specific users to whom you want to grant access. You can use the **Exchange Servers** group as criteria when you configure notification subscriptions. You can also use the **Exchange Servers** group as criteria for a report parameter.

Using Queues to Manage Work Items

In Service Manager, queues are used to group similar work items that meet specified criteria, for example, all incidents that are classified by analysts as E-mail incidents. All work items in a queue must be of the same type, such as incidents, change requests, activities, or trouble tickets. Queues use membership rules to determine which work items should be included in each queue. Queue membership rules are dynamic, and they are periodically recalculated to ensure that the queue membership list is current.

You can create a queue to group work items with a specific type or with a specific priority. You can then configure user roles to limit access to that queue to only specific users.

For incident escalation, you can use queues in various ways to speed the resolution of higher priority or common incidents. For example, you can configure Incident Management to automatically escalate specific incidents to a high-priority queue

For example, you can use queues as follows:

- In notifications, you can use a queue as criteria in a subscription to specify which work items to notify about.
- In security, you can use a queue in user role configuration to limit the scope of control that groups of users have over work items.

Note

When you delete a queue, the work items that are contained in the queue are preserved. You can delete a queue only if it is in an unsealed management pack.

Using Lists to Customize Forms

You can use lists in Service Manager to classify different objects, such as incidents, change requests, activities, or configuration items. A list represents a property of an object, and it includes one or more *list items*. Each list item represents a possible value for a property.

Lists are used in forms and dialog boxes throughout the Service Manager console. Lists and list items make it possible for users to select a value from a predefined list of values. When you use lists, you can customize the console to reflect the business practices of your organization. Additionally, Service Manager contains several predefined lists, such as the **Incident Classification** list.

For example, when you are creating an incident, you notice that **Printer Problems** is an option under **Classification Category**. At your company, some standard laser printers in your accounting department might be used as specialized check-writing printers. To better route incidents, you want printer-related incidents to be categorized as being either for standard laser printers or for check-writing printers. Because lists are customizable, you can add a list item, such as **Laser Printers** and **Check-Writing Printers**, to the **Classification Category** list when you create an incident. Optionally, you can build lists as a hierarchy; for example, laser printers and check-writing printers could be listed under printers. To do this, you can add **Laser Printer** and **Check-Writing Printer** list items to the **Incident Classification** list.

About List Items

In Service Manager, several default list items exist. It is important that you not delete the default list items. Each default list item is defined by a globally unique identifier (GUID). Some of the default management packs reference these list items by their GUID. If you delete a list item, some management packs or workflows might not work.

If the name of a default list item causes an issue in your environment, you can change the display name of the existing item but leave the GUID intact. For example, you can change the name of

the **Printing Problems** default list item to *Laser Printing Problems* if that is better in your environment.

See Also

How to Create a Group

How to Create a Queue

How to Edit a Queue

How to Add a List Item

How to Create a Group

Use the following procedures in System Center 2012 – Service Manager to create a new group (such as the **Exchange Servers** group) that includes the servers in your environment that are running Microsoft Exchange Server.

Note

We recommend that you create a Configuration Manager 2007 connector before you run this procedure. For more information, see Importing Data from Configuration Manager 2007.

To create a new group

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Groups**.
3. In the **Tasks** pane, under **Groups**, click **Create Group**. The Create Group Wizard starts.
4. On the **Before You Begin** page, click **Next**.
5. On the **General** page, do the following:
   a. Provide a name for the group, such as **Exchange Servers**.
   b. In the **Description** text box, type a description for the group. For example, type **All Exchange servers that require an update.**
   c. Under **Management pack**, make sure that an unsealed management pack is selected. For example, select **Service Catalog Generic Incident Request**. Then, click **Next**.
6. On the **Included Members** page, click **Add**.
7. In the **Select Objects** dialog box, in the **Filter by class** list, select a class, such as **Windows Computer**.
8. In the **Search by name** box, type the search criteria that you want to use to locate an object, and then click the filter (magnifying glass) button.
9. Select one or more items in the **Available Objects** list, and then click **Add**. For example, select all the Exchange servers in your organization.
10. Verify that the objects that you selected in the **Available Objects** list appear in the **Selected objects** list, and then click **OK**.

11. On the **Included Members** page, click **Next**.
12. Optionally, on the **Dynamic members** page, click the ellipsis (…) button to specify a type, such as **Windows Computer**, to build the dynamic members. Choose any property you want to build your criteria. For example, after you specify the **Windows Computer** type, select the **Principal Name** property, and then click **Add**. In the related text box, enter **woodgrove** so that all the computers whose principal name contains this text are included, and then click **Next**.
13. Optionally, on the **Subgroups** page, click **Add**, and then select the specific groups that you want as subgroups of this group. If any group that you want to select as a subgroup is from an unsealed management pack, that subgroup must be from the same management pack as the group that you are creating. Click **OK**, and then click **Next**.
14. Optionally, on the **Excluded Members** page, click **Add**, and then select the specific configuration items that you want to exclude from this group. Click **OK**, and then click **Next**.
15. On the **Summary** page, confirm the group settings that you made, and then click **Create**.
16. On the **Completion** page, make sure that you receive the following confirmation message, and then click **Close**:

    "The new group was created successfully."

To validate the creating of a new group

- Make sure that **Exchange Servers** appears in the **Groups** pane. If necessary, press the F5 key to refresh the Service Manager console view.

  In the **Tasks** pane, under the name of the group, click **View Group Members** to make sure that the Exchange servers appear in the **Group Members** window.

You can use a Windows PowerShell command to retrieve groups from Operations Manager and from Service Manager. For more information, see Get-SCSMGroup.

How to Create a Queue

You can create queues in System Center 2012 – Service Manager to create a grouping of related work items, such as incidents and change requests. For example, you can create a queue that you use for escalation, named **Exchange Send Problems Queue**, and then escalate that type of incident to that queue.

You can use the following procedure to create a queue.

To create a queue

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Queues**.
3. In the **Tasks** pane, click **Create Queue**.
4. Complete these steps to complete the Create Queue Wizard:

a. On the **Before You Begin** page, click **Next**.
b. On the **General** page, type a name in the **Queue name** box. For example, type **Exchange Send Problems Queue**.
c. Next to the **Work item type** box, click the ellipsis button (**…**). In the **Select a Class** dialog box, select a class, such as **Incident**, and then click **OK**.
d. In the **Management pack** list, select the unsealed management pack in which you want to store the new queue definition. For example, select **Service Manager Incident Management Configuration Library**. Then, click **Next**.
e. On the **Criteria** page, build the criteria that you want to use to filter work items for the queue, and then click **Next**. Only work items that meet the specified criteria will be added to that queue.

   For example, select the **Classification Category** property in the **Available Properties** area, and then click **Add**. In the list that was just added to the **Criteria** area, in the area that is now surrounded by a red box, select **E-Mail Problems**, and then click **Next**.
f. On the **Summary** page, click **Create** to create the queue.
g. On the **Completion** page, click **Close**.

To validate the creation of a queue

1. In the Service Manager console, verify that the new queue appears in the **Queues** pane.
2. In the **Tasks** pane, click **Properties**, and then verify that the queue appears as you defined it.

You can use a Windows PowerShell command to complete this task. For information about how to use Windows PowerShell to retrieve queues that are defined in Service Manager, see Get-SCSMQueue.

How to Edit a Queue

In System Center 2012 – Service Manager, you can use the following procedure to edit a queue.

To edit a queue

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Queues**.
3. In the **Queues** pane, select the queue that you want to edit, such as **Exchange Send Problems Queue**. Then, in the **Tasks** pane, click **Properties**.
4. In the **Queue Properties** dialog box, on the **General** and **Criteria** tabs, make the changes you want. For example, change the description of the queue.
5. Click **OK** to save the changes.

How to Add a List Item

In System Center 2012 – Service Manager, you can use these procedures to add a list item to an existing list and then validate it. For example, you can use this procedure to add a Laser Printer and Check-Writing Printer list item to the **Incident Classification** list.

To add list items to Service Manager lists

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, click **Lists**. The **Lists** pane displays all the existing lists.
3. Select the list to which you want to add a list item. For example, select the **Incident Classification** list. In the **Tasks** pane, under **Incident Classification**, click **Properties**.
4. In the **List Properties** dialog box, click **Printing Problems**, and then click **Add Child**. Notice that a new **List Value** list item is added.

   Note
   When you click **Add Item** or **Add Child**, a **Select management pack** dialog box might appear. If this dialog box appears, select the default management pack, select another unsealed management pack, or create a new management pack.
5. Click the new **List Value** list item. In the **Name** box, type a name for the new list item. For example, type **Laser Printer**. If you want, you can optionally type a description in the **Description** box.
6. Repeat steps 4 and 5 and create a new list item with the name **Check-Writing Printer**, and then click **OK**.

To validate the addition of a new list item

1. Select the same list again, click **Properties** in the **Tasks** pane, and then verify that the new list item appears.
2. In the Service Manager console, create a new incident, and then locate the new list item in the **Classification Category** list. For example, expand **Printer Problems**, and then locate the **Laser Printer** and **Check-Writing Printer** list items.

   For more information about creating a new incident, see the topic **How to Manually Create a New Incident** in the Operations Guide for System Center 2012 – Service Manager.

Using Runbooks in System Center 2012 - Service Manager

Runbooks in System Center 2012 – Service Manager and System Center 2012 - Orchestrator are used to automate procedures. The following topics provide details about the purpose and use of runbooks.

Runbook Topics

- About Runbooks in Service Manager

  Provides an overview of the purpose of runbooks in Service Manager.
- How to Create a Runbook Automation Activity Template

  Describes how to create a runbook automation activity template.
- How to View a Runbook

  Describes how to view a runbook.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Runbooks in Service Manager

To automate processes in System Center 2012, System Center 2012 - Orchestrator uses runbooks to automate procedures. Runbooks are visual representations of the procedures. The value that runbooks have is that they help ensure that Orchestrator automation is driven and tracked from System Center 2012 – Service Manager and that Service Manager interactions with other Service Manager products and non-Microsoft systems are much easier to implement.

Additionally, the Orchestrator workflow authoring interface is available for your custom Service Manager scenarios. Runbooks are imported into Service Manager using the Orchestrator connector. After the connector is synchronized, imported runbooks appear in the **Library** workspace under the **Runbooks** node in the Service Manager console, where you can view them and also create runbook automation activity templates.

About System Center 2012 - Orchestrator

System Center 2012 - Orchestrator is an automation platform for orchestrating and integrating IT tools to drive down the cost of datacenter operations, while improving the reliability of IT processes. Orchestrator enables IT organizations to automate best practices, such as those that are found in the Microsoft Operations Framework (MOF) and Information Technology Infrastructure Library (ITIL). This is achieved through workflow processes that coordinate Service Manager and other management tools to automate incident response, change and compliance, and service-life-cycle management processes.

Through its workflow designer, Orchestrator automatically shares data and initiates tasks in System Center 2012 components, including Operations Manager, Service Manager, Virtual Machine Manager, System Center 2012 - Configuration Manager, Active Directory Domain Services (AD DS), and non-Microsoft tools. Orchestrator workflow automates IT infrastructure tasks, while Service Manager workflow provides automation of human workflow. The combined

offering ensures repeatable, consistent results by removing the latency associated with manual coordination service delivery. Service Manager and Orchestrator enable integration, efficiency, and business alignment of datacenter IT services by:

- Automating processes and enforcing best practices for incident, change, and service-life-cycle management.
- Reducing unanticipated errors and service delivery time by automating tasks across responsibility groups within your IT organization.
- Integrating System Center with non-Microsoft tools to enable interoperability across the datacenter.
- Orchestrating tasks across systems for consistent, documented, and compliant activity.

See Also

Using Runbooks in System Center 2012 - Service Manager

How to Create a Runbook Automation Activity Template

After you import runbooks into System Center 2012 – Service Manager using the Orchestrator connector from System Center 2012 - Orchestrator, you can create a runbook automation activity template to map parameters in Orchestrator to corresponding parameters in Service Manager.

As an example, you can implement a new request offering using an Orchestrator runbook to automate it. Then, you can go to the Runbooks view in the Library workspace, select a runbook, and create a runbook automation activity template. You can go to the templates view and verify that the template is created. You can then add the Orchestrator activity template to a service request template and create the request offering. You then can then map the runbook template to a different runbook with the same inputs and outputs if you find that you need to fix a problem or improve the process.

Important

If you have extended root classes such as service request or release record, then you can map runbook activity parameter to extended properties only if the runbook activity template and service request templates are saved in same management pack where the definition extension is located.

To create a runbook automation activity template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, click **Runbooks**.
3. In the **Runbooks** view, select a runbook.
4. In the **Tasks** pane, under **<RunbookName>**, click **Create Runbook Automation Activity Template** to open the **Create Template** dialog box.
5. In the **Name** box, type a name for the template.
6. Optionally, in the **Description** box, type a description for the template.
7. If necessary, select an unsealed management pack to save the template to, and then

click **OK**. You will use this management pack later to retrieve the runbook automation activity template from another work item template, such as a service request template.

8. In the Runbook Activity Template: <TemplateName> form, on the **General** tab, type information for **Title**, **Description**, **Area**, **Stage**, **Assigned To**, and **Designer**.
9. Ensure that **Is Ready for Automation** is selected.
10. Select the **Runbook** tab, and then under **Parameter Mapping**, note that the parameters from the runbook are mapped to generic properties—for example, Parameter1, Parameter2, and so on—of the runbook activity class. The **Type** column specifies whether the parameters are inputs or outputs. You can also type default values for each parameter using **Edit Mapping**.
11. For any parameter, click **Edit Mapping**.
12. Expand **Object**, and then click **Id**. This ID value will be used by the Orchestrator runbook to find the particular runbook activity that is being executed. Click **Close**.
13. Click **OK** to close the form and create the template.

How to View a Runbook

After you import runbooks from System Center 2012 - Orchestrator into System Center 2012 – Service Manager, you can open the runbook in the Service Manager console to ensure that it contains the parameters you want to use in an automation activity template in Service Manager.

Note

This procedure requires Windows Internet Explorer with Microsoft Silverlight installed.

When you view the runbook, you can perform basic actions with the runbook, such as viewing the summary, jobs, instances, and definition of the runbook. You can also start and stop the runbook.

To view a runbook

1. In the Service Manager console, select **Library**.
2. In the **Library** pane, select **Runbooks**.
3. In the **Runbooks** view, select a runbook.
4. In the **Tasks** pane under **<RunbookName>**, click **View Runbooks** to open the runbook in Internet Explorer.

See Also

Using Runbooks in System Center 2012 - Service Manager

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

This section provides an overview of key concepts for chargeback reports in System Center 2012 – Service Manager SP1 and System Center 2012 R2 Service Manager. This section also contains procedures that you can use to install and configure chargeback reports. After you have installed and configured chargeback reports, see the installing and configuring chargeback reports, see the Managing Chargeback Reports topic in the Operations Guide for System Center 2012 – Service Manager.

Installing and Configuring Chargeback Reports Topics

- About Chargeback Reports

  Provides an overview of key concepts for chargeback reports.
- Chargeback Report Requirements

  Provides an overview of requirements that must be met before you install chargeback reports.
- How to Install Chargeback Reports

  Describes how to install chargeback reports.
- How to Create or Modify a Price Sheet

  Describes how to view and use chargeback reports.
- How to Publish and Unpublish a Price Sheet

  Describes how to publish and unpublish a price sheet.
- How to Assign or Remove a Default Price Sheet for a Selected Cloud

  Describes how to assign or remove a default price sheet for a cloud.
- How to Override a Default Price Sheet for a Specific VMM User Role

  Describes how to override a default price sheet for a VMM user role.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Chargeback Reports

As traditional IT transitions into a cloud-optimized IT, service providers are facing a new set of challenges that places a high demand on them. One of the goals of System Center 2012 is to enable and help you, the service provider, to manage the transition, and to help you succeed in your offerings.

In traditional IT, infrastructure was largely physical, service level agreements (SLAs) were typically periods of weeks and months, and capacity was owned and managed by the consumers. However, this is no longer true. With the arrival of centrally pooled resources, on-demand self-service, and short SLAs, service consumers can continue their old habits, which are to over-subscribe and underutilize, without having to carry the burden of managing the acquired capacity. If not managed properly, the ability of the service provider can be compromised in these situations.

In System Center, chargeback is one of the tools that help you communicate with business units about how they consume capacity. This helps you by utilize existing investments, proportionate to your customer's requests. System Center components help you manage the following processes:

- Quotas
- Leases
- Approvals
- Chargeback or showback

The theme of chargeback is cloud based pricing, where each cloud has its own price, based on SLA. Most often, you'll have many clouds with various SLAs for the clouds for different business units or organizations. Chargeback uses a price sheet, or rate card, for each cloud. This means you can have one price represented in a price sheet that contains various clouds addressing one SLA, and you can have another price sheet for a different SLA.

Specifically, Chargeback in Service Manager uses information discovered from the Operations Manager CI connector about the Virtual Machine Manager fabric that you manage. The private cloud information from Virtual Machine Manager, such as clouds and virtual machines, is what helps define a successful private cloud by offering centrally pooled resources that are metered and charged based on consumption.

Price sheets, or rate cards, are created in Service Manager for Virtual Machine Manager clouds. The clouds are then assigned to prices sheets. For example, you might have price sheets that are associated to silver and bronze clouds in order to differentiate levels of service.

Service Manager comes with a sample report, but its reporting infrastructure is OLAP cube-based, so you can easily create your own reports. You can easily customize the sample report with colors, logos, or whatever you can think of that will best suit your needs. You can use the OLAP cube information presented in the Data Warehouse workspace to easily create a simple pivot table in Microsoft Excel. After you select fields you like, you can format the data any way you like just like you would any other information in Excel.

It's important to let customers know that IT resources are limited in their capacity. You can use chargeback or showback reports to show resource utilization and the associated costs to influence consumption behaviors.

Operations Manager Requirements

Before you can use chargeback reports, you must create and synchronize an Operations Manager CI connector so that Operations Manager discovers virtual machine resources from Virtual Machine Manager 2012 SP1. Earlier versions of Virtual Machine Manager are not

supported with Chargeback. During this process, you must synchronize the VMM.2012.Discovery management pack. For more information about creating and synchronizing an Operations Manager CI connector, see How to Create a System Center Operations Manager Connector. The following object properties are imported into Service Manager using the connector:

- virtual machine CPU count
- virtual machine memory
- virtual machine storage
- virtual network interface cards
- virtual disks
- virtual machines – this is used to collect a fixed price for virtual machines other than for virtual machine components
- clouds – used to collect cloud membership price for clouds other than virtual machine or virtual machine component costs

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

Chargeback Report Requirements

The following information describes the steps you need to consider before installing System Center 2012 – Service Manager SP1 and chargeback reports.

1. Review the information in the Deployment Guide for System Center 2012 - Service Manager before you install System Center 2012 – Service Manager SP1.
2. Review hardware and software requirements for System Center 2012 Service Pack 1 (SP1) for Service Manager in the **Hardware Requirements for System Center 2012 SP1 - Service Manager** and **Software Requirements for System Center 2012 SP1- Service Manager** topics.
3. Install System Center 2012 – Service Manager SP1.

After you have reviewed and met requirements for chargeback reports, you're ready to install chargeback files, as described in detail in the How to Install Chargeback Reports topic.

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

How to Install Chargeback Reports

Chargeback reports in System Center 2012 – Service Manager consist of various files such as management pack files, Windows PowerShell scripts to import the management pack files, and a Microsoft Excel sample report. The first of the following procedures imports Service Manager management pack files and the second procedure imports management pack files on the Operations Manager management server.

All files that comprise chargeback reports are located in the Service Manager installation folder in the Chargeback subfolder. For example, if you installed Service Manager in C:\Program Files, then all chargeback report files will be located in C:\Program Files\Microsoft System Center 2012\Service Manager\Chargeback

You must have System Center 2012 – Service Manager SP1 or System Center 2012 R2 Service Manager installed and have administrative credentials on the server hosting the Service Manager and Operations Manager management servers in order to install chargeback report files. Additionally, System Center 2012 R2 Operations Manager must monitor System Center 2012 R2 Virtual Machine Manager servers.

For System Center 2012 R2 Service Manager only: The installation procedure below uses the ImportToSM.ps1 PowerShell script that uses parameters described in the following table. If you run the script without specifying any parameters, you are prompted for them.

Parameter	Description
omServer	Name of the Operations Manager server
omUsername	User name of the account that has administrative access to the Operations Manager management server
omPassword	Password of the account that has administrative access to the Operations Manager management server
smUsername	User name of the account that has administrative access to the Service Manager management server
smPassword	Password of the account that has administrative access to the Service Manager management server

Note

When you try to use chargeback after you have upgraded to System Center 2012 R2 Service Manager, your Operations Manager CI connector might stop synchronizing new System Center 2012 R2 Virtual Machine Manager objects, such as VMM clouds, if the VMM Server was upgraded to System Center 2012 R2 Virtual Machine Manager. This occurs because Service Manager does not have the correct version of the VMM management packs. Additionally, installing chargeback report files to the System Center 2012 R2 Operations Manager management server might fail after you upgrade System Center 2012 R2 Service Manager because the Dependencies folder does not contain the required management pack files. Use the following procedures to prepare for chargeback reports. If you have upgraded to Service Manager, see After Upgrading to System Center

2012 R2 - Service Manager for more information about preparing management pack files for Service Manager.

After you have installed chargeback report files on the Operations Manager and Service Manager management servers and configured the Operations Manager CI connector, you are ready to use chargeback report features.

To install chargeback report files on the Operations Manager management server

1. Log on to the Operations Manager management server.
2. In the Chargeback folder, copy the subfolder named Dependencies from the Service Manager management server to the Operations Manager management server.
3. On the Operations Manager management server, start Windows PowerShell and then navigate to the Dependencies folder. For example, type **cd Dependencies**.
4. If you have not already set execution policy to remotesigned, then type the following command, and then press ENTER:

   ```
   Set-ExecutionPolicy -force RemoteSigned
   ```

5. Type the following command, and then press ENTER to run the PowerShell script that imports chargeback management packs and that add chargeback functionality to Operations Mananger:

   ```
   .\ImportToOM.ps1
   ```

6. After the script has completed running, type **exit**, and then press ENTER to close the **Administrator: Windows PowerShell** window.
7. Ensure that Operations Manager is connected to Virtual Machine Manager, as described at How to Connect VMM with Operations Manager.
8. Ensure that Operations Manager has discovered information from virtual machine manager such as virtual network interface cards, virtual hard disks, clouds, and virtual machines.

To install chargeback reports on the Service Manager management server

1. Log on to the System Center 2012 – Service Manager SP1 management server.
2. On the computer where you want to run Windows PowerShell, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Service Manager**, and then click **Service Manager Shell**.
3. If you have not already set execution policy to remotesigned, then type the following command, and then press ENTER:

   ```
   Set-ExecutionPolicy -force RemoteSigned
   ```

4. Navigate to the Chargeback folder. For example, type **cd chargeback**.
5. Type the following command, and then press ENTER to run the PowerShell script that imports chargeback management packs and that add chargeback functionality to Service Manager:

   ```
   .\ImportToSM.ps1
   ```

6. After the script has completed running, type **exit**, and then press ENTER to close the **Administrator: Windows PowerShell** window.
7. In the Service Manager console, click **Data Warehouse**, expand the **Data Warehouse** node, and then click **Data Warehouse Jobs**.
8. In the list of data warehouse jobs, select **MPSyncJob** and then in the Task list, click **Resume**.
9. Configure the Operations Manager CI connector and ensure that Service Manager has discovered the virtual machine information from Operations Manager. For more information about creating and synchronizing an Operations Manager CI connector, see How to Create a System Center Operations Manager Connector.

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

How to Create or Modify a Price Sheet

Price sheets in System Center 2012 – Service Manager allow you to define price policies on existing private cloud objects that are discovered from the Operations Manager CI connector. You can associate one or more private clouds to a price sheet. After association, price information contained in the price sheet is shown in OLAP cubes and in a sample Excel report. You can use the OLAP cube data to create your own customized reports using various reporting solutions such as SQL Server Reporting Services, SQL Server Analysis Services tools, and Microsoft Excel. Additionally, you can modify the sample Excel report for your organization's needs.

Although you can create multiple price sheets without publishing them, you must publish a price sheet before you can associate cloud objects to the price sheet.

To create a price sheet

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Chargeback**, expand **Infrastructure**, expand **Price Sheets**, and then select **All Price Sheets**.
3. In the **Tasks** pane under **All Price Sheets**, click **Create Price Sheet**.
4. On the **General** tab, complete these steps:
   a. In the **Name** box, type a title for the price sheet. For example, type **Gold Price Sheet**.
   b. Optionally, in the **Description** box, you can type a description of the price sheet. For example, type **The gold price sheet describes our highest level of service available and is more costly than others offered.**
   c. You can optionally publish the price sheet using the **Publish** task in the Tasks list of the form. Publishing the price list enables you to assign cloud objects to the price list.
5. On the **Price** tab, complete these steps:
   a. In the **VM Base Price per day** box, type the daily base price value of the virtual

machine. For example, type **22.55**.

b. In the **Cloud Membership Price per day** box, type the base price value for membership in the cloud. For example, type **10.20**.

c. In the **VM CPU Price per Core/day** box, type the price value of the CPU core in the virtual machine that is included in the virtual machine. For example, type **1.20**.

d. In the **VM Memory Price per GB/day** box, type the price value of each GB of memory in the virtual machine that is included in the associated cloud. For example, type **.30**.

e. In the **VM Storage Price per GB/day** box, type the base value of each GB of storage space in the virtual machine that is included in the associated cloud. For example, type **.10**.

f. In the **Highly Available VM Price per day** box, type the price value for each virtual machine that is highly available. For example, type **1.10**.

g. In the **Static IP Price per day** box, type the price value for each static IP address for virtual machines. For example, type **.05**.

h. In the **Expanding VHD Price per day** box, type the price value expanding VHDs. For example, type **.55**.

i. You can optionally publish the price sheet using the **Publish** task in the Tasks list of the form. Publishing the price list enables you to assign cloud objects to the price list.

6. If you have published the price sheet, you can optionally assign clouds to the price list using the Assigned Clouds **Price** tab by completing these steps:

   a. Click **Add**, to open the **Select objects** dialog box.

   b. In the list of **Private Cloud** objects, select one or more private cloud objects and then click **Add** to add them to the **Selected objects** list.

   c. Click **OK** to close the **Select objects** dialog box and assign the cloud objects to the price sheet.

   d. Click **OK** to close the price sheet form.

To modify a price sheet

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Price Sheets**, and then select a view that contains a price sheet that you want to modify.
3. In the list of price sheets, select the one you want to modify and then in the **Tasks** pane under **Tasks**, click **Edit**.
4. On the **General** tab, complete any of the following steps that you want to in order to update the price sheet:

   a. In the **Name** box, update the title for the price sheet. For example, type **Silver Price Sheet**.

   b. In the **Description** box, you can update the description of the price sheet. For example, type **The sliver price sheet describes our highest level of service available and is more costly than others offered.**

   c. You can optionally publish the price sheet using the **Publish** task in the Tasks list of

the form. Publishing the price list enables you to assign cloud objects to the price list.

5. On the **Price** tab, complete any of the following steps that you want to in order to update the price sheet:
   a. In the **VM Base Price per day** box, update the daily base price value of the virtual machine. For example, type **11.44**
   b. In the **Cloud Membership Price per day** box, update the base price value for membership in the cloud. For example, type **9.10**
   c. In the **VM CPU Price per Core/day** box, update the price value of the CPU core in the virtual machine. For example, type **0.60**
   d. In the **VM Memory Price per GB/day** box, update the price value of each GB of memory in the virtual machine. For example, type **.15**
   e. In the **VM Storage Price per GB/day** box, update the base value of each GB of storage space in the virtual machine. For example, type **.05**
   f. In the **Highly Available VM Price per day** box, update the price value for each virtual machine that is highly available. For example, type **.90**.
   g. In the **Static IP Price per day** box, update the price value for each static IP address for virtual machines. For example, type **.03**.
   h. In the **Expanding VHD Price per day** box, update the price value for expanding VHDs. For example, type **.80**.
   i. You can optionally publish the price sheet using the **Publish** task in the Tasks list of the form. Publishing the price list enables you to assign cloud objects to the price list.
6. If you have published the price list, you can optionally assign or remove clouds to the price list using the Assigned Clouds **Price** tab by completing these steps:
   a. Click **Add**, to open the **Select objects** dialog box.
   b. If you want to add private cloud objects, in the list of **Private Cloud** objects, select one or more private cloud objects and then click **Add** to add them to the **Selected objects** list.
   c. Click **OK** to close the **Select objects** dialog box and assign the cloud objects to the price sheet.
   d. If you want to remove private cloud objects, in the list of **Private Cloud** objects, select one or more private cloud objects and then click **Remove**.
   e. Click **OK** to close the price sheet form.

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

How to Publish and Unpublish a Price Sheet

You must have created a price sheet and saved it before you can publish it. After you publish a price sheet, you can assign private cloud objects to the price sheet. For more information about publishing a price sheet, see How to Create or Modify a Price Sheet.

Note

You can unpublish a price sheet only when it does not have cloud objects assigned to it or if a VMM cloud user role has not been assigned.

To publish a price sheet

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Price Sheets**, and then select a price sheet view that contains one that you want to publish.
3. In the list of price sheets, select the price sheet with Draft status that you want to publish.
4. In the **Tasks** pane click **Publish**.

To unpublish a price sheet

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Price Sheets**, and then select a price sheet view that contains one that you want to unpublish.
3. In the list of price sheets, select the price sheet with Published status that you want to unpublish.
4. In the **Tasks** pane click **Unpublish**.

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

How to Assign or Remove a Default Price Sheet for a Selected Cloud

After Service Manager has discovered cloud objects from the Operations Manager CI connector, you can assign an existing price sheet that applies default price values to all the resources of the cloud. This process is useful when you have many virtual machines so that you do not have to define prices for all the individual virtual machine parts. Once the default price sheet is assigned to a cloud, you can override the default values, on a per-user basis. For more information about overriding default prices, see How to Override a Default Price Sheet for a Specific VMM User Role.

To assign a default price sheet to a selected cloud

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Chargeback**, expand **Clouds**, and then select **All Clouds**.
3. In the list of clouds, select one that you want to assign a price sheet to and then under Tasks, click **Assign Price Sheet**.
4. In <CloudName> form under **Default Cloud Price Sheet**, in the Action column, click

Assign Price Sheet.

> **Note**
> If a cloud previously had a price sheet assigned, then assigning a new one automatically unassigns the price sheet that was used previously.

5. In the **Select objects** dialog box, select a price sheet that you want to assign and then click **OK**.
6. Click **OK** to close the <CloudName> form.

> **Note**
> If a cloud does not have a price sheet assigned, all virtual machines in the cloud will have a price of zero in chargeback reports.

To remove a default price sheet from a selected cloud

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Chargeback**, expand **Clouds**, and then select **All Clouds**.
3. In the list of clouds, select one that you want to remove the default price sheet from to and then under Tasks, click **Edit**.
4. In <CloudName> form under **Default Cloud Price Sheet**, click **Remove**.
5. Click **OK** to close the <CloudName> form.

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

How to Override a Default Price Sheet for a Specific VMM User Role

After Service Manager has discovered cloud objects from the Operations Manager CI connector, you can assign an existing price sheet that applies default price values to all the resources of the cloud. This process is useful when you have many virtual machines so that you do not have to define prices for all the individual virtual machine parts. Once the default price sheet is assigned to a cloud, you can override the default values, on a per-user basis. For more information about assigning a default price sheet to a cloud, see How to Assign or Remove a Default Price Sheet for a Selected Cloud.

To override a default price sheet for a specific VMM user role

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Chargeback**, expand **Clouds**, and then select **All Clouds**.
3. In the list of clouds, select one that you want to assign a price sheet to and then under Tasks, click **Assign Price Sheet**.

4. In <CloudName> form under **User Role Price Sheet Overrides**, click **Add**.
5. In the **Select objects** dialog box, select a VMM user role that you want to override the default price sheet with and click **Add** and then click **OK**.
6. Under **User Role Price Sheet Overrides** scroll to the right and click **Assign Price Sheet** and then select a price sheet that is applied for the selected user only, and then click **OK**.

   Note
   If a cloud previously had a price sheet assigned, then assigning a new one automatically unassigns the price sheet that was used previously.
7. Click **OK** to close the <CloudName> form.

See Also

Installing and Configuring Chargeback Reports in System Center 2012 - Service Manager

User Interface Customization in System Center 2012 - Service Manager

The sealed management packs in Service Manager contain, among other things, views, list items, and templates. Because these items are in a sealed management pack, they cannot be edited or changed. With the release of System Center 2012 – Service Manager, you have the option of hiding views. You can now duplicate list items and templates, saving the duplicates into an unsealed management pack, and because the duplicates are in an unsealed management pack, you can edit the properties of the list item or template using the Service Manager console.

User Interface Customization Topics

- How to Customize a View

  Describes how to customize a view.
- How to Customize a List Item

  Describes how to customize a list item.
- How to Customize a Template

  Describes how to customize a template.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Customize a View

The **Failed Service Requests** view in System Center 2012 – Service Manager is in a sealed management pack. In this example, you will create a duplicate of this view, save it into an unsealed management pack, and then edit the new view by changing its name to **New Failed Service Requests**. You will finish this exercise by hiding the original Failed Service Requests view. As an administrator, you will still see the hidden view.

To customize a view

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Service Request Fulfillment**.
3. Right-click **Failed Service Requests**, and then click **Duplicate View**.
4. In the **Select management pack** dialog box, accept the default management pack, **Service Manager Service Request Configuration Library**, and then click **OK**.
5. Right-click **Failed Service Requests – Copy**, and then click **Edit View**.
6. In the Edit Failed Service Requests – Copy Wizard, in **Name**, type a new name for this view. For example, type **New Failed Service Requests**, and then click **OK**.
7. Right-click **Failed Service Requests**, and then click **Hide View**.

See Also

User Interface Customization in System Center 2012 - Service Manager

How to Customize a List Item

The items in a list in a sealed management pack in System Center 2012 – Service Manager cannot be changed. In this example, you will add a list item (phone) to the **Service Request Source** list and save it into an unsealed management pack, and then edit the new view by changing its name to **New Failed Service Requests**. You will finish this exercise by hiding the original Failed Service Requests view. As an administrator, you will still see the hidden view.

To customize a list item

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Lists**.
3. In the **Lists** pane, click **Service Request Source**.
4. In the **Tasks** pane, in the **Service Request Source** area, click **Properties**.
5. In the **List Properties** dialog box, click **Add Item**.
6. In the **Select management pack** dialog box, accept the default management pack, **Service Manager Service Request Configuration Library**, and then click **OK**.
7. In the **List Properties** dialog box, click **List Value**.
8. In the **Name** field, type **Phone**, and then click **OK**.

See Also

User Interface Customization in System Center 2012 - Service Manager

How to Customize a Template

Templates in a sealed management pack in System Center 2012 – Service Manager cannot be changed. In this example, you will create a copy of the Default Service Request Template and save the copy in an unsealed management pack. You will then start a Create Template Wizard for the copy you made.

To customize a template

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Library**, and then click **Templates**.
3. In the **Templates** pane, click **Default Service Request**.
4. In the **Tasks** pane, under **Default Service Request**, click **Create a Copy**.
5. In the **Select management pack** dialog box, accept the default management pack, **Service Manager Service Request Configuration Library**, and then click **OK**.
6. In the **Templates** pane, click **Copy of Default**.
7. In the **Tasks** pane, under **Copy of Default Service Request**, click **Properties**.
8. In the **Create Template** dialog box, in the **Name** field, type a new name for this template, and then click **OK**.
9. Finish the steps in the Service Request Template Wizard to customize this template for your needs, and when you are finished, click **OK**.

Managing User Roles in System Center 2012 - Service Manager

This section provides an overview of user roles in System Center 2012 – Service Manager. It includes procedures that you can use to work with user roles.

You can find a complete list of user roles in Service Manager at Appendix A - List of User Role Profiles in System Center 2012 - Service Manager.

Managing User Roles Topics

- About User Roles

  Provides an overview of user roles.
- How to Add a Member to a User Role

  Describes how to add a member to an existing user role.
- How to Create a User Role

Describes how to create a user role.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About User Roles

In your organization, some employees are responsible for supporting hardware, such as portable computers and servers. Some of the employees are allowed to create and update configuration items but not delete them, whereas others are allowed to create, update, and delete configuration items.

In System Center 2012 – Service Manager, the security rights that allow users to access or update information are defined in a user role profile. A user role profile is a named collection of access rights, and it usually corresponds to an employee's business responsibilities. Each user role profile controls access to such artifacts as knowledge articles, work items (incidents, change requests), authoring, administration, and other credentials. Think of user role profiles as defining what you are allowed to do.

In the future, managers at your organization may decide to separate the group of employees who maintain configuration items into two groups: those who handle configuration items for desktop computers and those who handle configuration items for portable computers. They want to retain these two user role profiles, one profile that can create and edit but not delete configuration items, and another profile that can create, edit, and delete configuration items. You would define these user role profiles with different scopes, one for desktops and one for portable computers. If user role profiles define what you are allowed to do, think of scopes as defining what items you are allowed to modify. The combination of a user role profile and a scope is called a user role.

Understanding User Roles in Service Manager

In Service Manager, when you click **Administration**, expand **Security**, and then click **User Roles**, a **User Roles** pane displays a list of user roles. Each of these user roles has been configured with a user role profile and an undefined scope. Because the scope is undefined for these user roles, they can exercise their user profiles on all management packs, queues, groups, tasks, views, and form templates. The following table lists the default user roles, their associated user role profiles, and scope.

User role	User role profile	Scope
Activity Implementers	Activity Implementer	Global
Administrators	Administrator	Global

User role	User role profile	Scope
Advanced Operators	Advanced Operator	Global
Change Initiators	Change Initiator	Global
End Users	End User	Global
Read-Only Operators	Read-Only Operator	Global
Authors	Author	Global
Problem Analysts	Problem Analyst	Global
Workflows	Workflow	Global
Incident Resolvers	Incident Resolver	Global
Change Managers	Change Manager	Global
Report Users	Report User	Global
Release Managers	Release Manager	Global
Service Request Analysts	Service Request Analyst	Global

Note

The Service Manager Report Users user role is available only after you register with the Service Manager data warehouse and after the Data Warehouse navigation button is available. To view the Service Manager Report Users user role, click **Data Warehouse**, expand **Security**, and then click **User Roles**.

Example

For example, say that you want to define one security access that allows users to create and edit, but not delete, configuration items and another security access that allows users to create, edit, and delete configuration items. Appendix A, at the end of this guide, lists the user role profiles and their associated artifacts. The following table shows user role profiles as they relate to configuration items.

User role profile	Create configuration items	Update configuration items	Delete configuration items
Report User	No	No	No
End User	No	No	No
Read-Only Operator	No	No	No
Activity Implementer	No	No	No

User role profile	Create configuration items	Update configuration items	Delete configuration items
Change Initiator	No	No	No
Incident Resolver	No	No	No
Problem Analyst	No	No	No
Change Manager	No	No	No
Advanced Operator	Yes	Yes	No
Author	Yes	Yes	No
Workflow	Yes	Yes	No
Administrator	Yes	Yes	Yes

Using the previous table, you can see that the Advanced Operators user role profile can create and update, but not delete, configuration items. The Administrators user role profile can create, update, and delete configuration items. The members of the asset management team who are allowed to create and update, but not delete, configuration items are made members of the predefined Service Manager Advanced Operators profile. The members of the asset management team who are allowed to create, edit, and delete configuration items are made members of the Administrators profile.

As a best practice, assume that members of the asset management team might change. You should create two groups in Active Directory Domain Services (AD DS) and make those groups members of the Advanced Operators and Administrators profiles. Then, as members change, users are added and removed from the Active Directory group, and no changes have to be made in Service Manager.

In the future, if you break the asset management team into two groups, one for desktops and the other for laptops, you can create your own user role by using the same user role profiles, but with different scopes.

Why Some User Roles Cannot Be Created

When you are creating a user role, notice that three user roles are not available: Administrator, Report User, and Workflows. These three user roles are created and populated during Setup, and, generally speaking, these user roles are used by Service Manager. The following sections describe each of these user roles.

Administrator

The Administrator user role is global in scope; therefore, there is no reason for creating another user role of this type.

Report User

The Report User user role has one purpose in Service Manager: to find the computer hosting Microsoft SQL Server Reporting Services (SSRS) for the user at a Service Manager console. When a user at a Service Manager console tries to run a report, a query is made to the Service Manager management server seeking the computer that is hosting the data warehouse management server. The Service Manager console then queries the data warehouse management server seeking the name of the computer hosting SSRS. With that information, the Service Manager console connects to SSRS. The singular purpose of the Report User user role is to make these queries. After the Service Manager console connects to the SSRS, the credentials of the user running the console grant access as defined on the SSRS. Because of the narrow purpose of this user role, there is no reason for creating another user role.

Workflows

Workflows might have to read and write to the Service Manager database. During Setup, you are asked to provide credentials for the Workflows user role, and this user role performs the required actions on the Service Manager database. Like the Report User user role, the narrow purpose of the Workflow user role means there is no reason for creating other user roles.

See Also

How to Add a Member to a User Role

How to Create a User Role

How to Add a Member to a User Role

In System Center 2012 – Service Manager, you can assign users to a user role to define what they can do.

In this example, you have to add members of an asset management team who can create and update, but not delete, configuration items to the user role. Looking at the “Configuration Items” section of Appendix A - List of User Role Profiles in System Center 2012 - Service Manager in this document, you see that the Advanced Operators user role profile provides what you need regarding permissions for this team. At this time, all members of the asset management team are responsible for every asset in the company; therefore, they require unlimited scope.

Use the following procedures to add a user to the Service Manager Advanced Operators user role and then validate the assignment of the user to the user role.

To assign a user to a user role

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Security**, and then select **User Roles**.
3. In the **User Roles** pane, double-click **Advanced Operators**.
4. In the **Edit User Role** dialog box, click **Users**.
5. On the **Users** page, click **Add**.

6. In the **Select Users or Groups** dialog box, type the name of a user or group that you want to add to this user role, click **Check Names**, and then click **OK**.
7. In the **Edit User Role** dialog box, click **OK**.

To validate the assignment of a user to a user role

- Log on to the Service Manager console as one of the users assigned to the user role. Verify that you cannot access data for which you do not have access rights, as specified in the user roles.

You can use a Windows PowerShell command to view users. For information about how to use Windows PowerShell to retrieve users that are defined in Service Manager, see Get-SCSMUser.

How to Create a User Role

Use the following procedures to create a user role and assign users to that role in System Center 2012 – Service Manager and then validate the creation of the user role.

To create a user role

1. In the Service Manager console, select **Administration**.
2. In the **Administration** pane, expand **Security**, and then select **User Roles**.
3. In the **Tasks** pane under **User Roles**, select **Create User Role**, and then select the user role profile that you want to use for this user role, such as **Author**.
4. Complete the **User Role Wizard** by doing the following:
   a. On the **Before You Begin** page, click **Next**.
   b. On the **General** page, enter a name and description for this user role, and then click **Next**.
   c. On the **Management Packs** page, start to filter the scope of the data that you want to assign access to. Select the management packs that contain the data that you want to assign access to, such as **Incident Management Library**. Click **Next**.
   d. On the following pages, all the classes, queues, groups, tasks, views, and form templates that are available for the specified user role from the specified management packs, are displayed. You can select specific items on these pages to further limit the set of data that access is assigned to.

      Important
      The groups and the queues lists are not filtered—all groups and queues from all management packs are listed. If you select **Select all queues** on the **Queues** page, on the **Groups** page, **Select all Groups** is selected automatically. In addition, by default, no groups have been created. You have to create a group if you want to limit scope by group.

   e. On the **Users** page, click **Add**, and use the **Select Users or Groups** dialog box to

select users and user groups from Active Directory Domain Services (AD DS) for this user role, and then click **Next**.

f. On the **Summary** page, make sure that the settings are correct, and then click **Create**.

g. On the **Completion** page, make sure that **The user role was created successfully** appears, and then click **Close**.

To validate the creation of a user role

1. In the Service Manager console, verify that the newly created user role appears in the middle pane.
2. Log on to the Service Manager console as one of the users assigned to the user role. Verify that you cannot access data for which you do not have access rights, as specified in the user role.

You can use Windows PowerShell commands to complete these and other related tasks, as follows:

- For information about how to use Windows PowerShell to create a new user role in Service Manager, see New-SCSMUserRole.
- For information about how to use Windows PowerShell to retrieve user roles that are defined in Service Manager, see Get-SCSMUserRole.
- For information about how to use Windows PowerShell to set the UserRole property for a Service Manager user, see Update-SCSMUserRole.
- For information about how to use Windows PowerShell to remove a user role from Service Manager, see Remove-SCSMUserRole.

Managing Run As Accounts in System Center 2012 - Service Manager

During the setup of System Center 2012 – Service Manager, you specified credentials for the workflow and service accounts, for Microsoft SQL Server Analysis Services, and for SQL Server Reporting Services (SSRS). If, because of the configurations of password security requirements used in your organization, these passwords expire, you must update the new passwords in Service Manager. In addition, if you decide that the user names must change, you also must change them in Service Manager. This section describes how to make those changes.

It is a best practice never to delete Run As accounts from the Service Manager console. The Service Manager management pack monitors Run As accounts. At regular intervals, the Health service attempts to log on as the Run As accounts. If this fails, Event ID 7000 is invoked that causes an alert. The best way to avoid this issue is never to delete Run As accounts from the Service Manager console. You can reuse existing Run As accounts by changing their name or credentials. If you want to stop using a Run As account, you can change its credentials to Local System and change the name to something easy to remember, such as "Inactive".

Managing Run As Accounts Topics

- How to Change the User Credentials for the Operational Database Account

  Describes how to update the Operational System Run As account if the user name and password has changed.
- How to Change the Password for the Operational Database Account

  Describes how to update the Operational System Run As account if only the password has changed.
- How to Change the Workflow Run As Account Credentials

  Describes how to update the workflow account if either the user name or password has changed.
- How to Change the Credentials for SQL Server Analysis Services Account

  Describes how to update the SQL Server Analysis account if either the user name or password has changed.
- How to Change the Credentials for SQL Server Reporting Services Account

  Describes how to update the SQL Server Reporting Services account if either the user name or password has changed.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Change the User Credentials for the Operational Database Account

If the user account for the Operational Database Account in System Center 2012 – Service Manager changes, you must make the following changes:

1. Add the new account to the Service Manager Administrators user role for both the Service Manager and data warehouse management servers
2. Create a SQL Server logon account for the new user on computers hosting Service Manager databases. On the computer hosting the Service Manager database, assign the new user to the skd_users and configsvc_users roles.
3. Make the new account a local administrator on the Service Manager computers.
4. Make the new user account the logon account for the Service Manager Data Access Service and Service Manager Management Configuration services, and then restart these services.

   Note

   The logon account for the Service Manager Management service is always the local system account and must not be changed.

5. Restart the Service Manager Management service.
6. Make the new user the Operational Run As account.

Use the following procedures to make these changes in Service Manager.

Important
Do not configure the Operational Database Account to use the Network Service account.

To add the user to the local administrators account

1. Add the new user as a member of the Administrators local group in Windows on the computers hosting the following:
   - Service Manager management server
   - Data warehouse management server
   - Self-Service Portal
   - Service Manager database
   - Data warehouse databases

To add the user to the Administrators user role

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Security**, and then click **User Roles**.
3. In the **User Roles** pane, click **Administrators**.
4. In the **Tasks** pane, click **Properties**.
5. In the Edit User Role Wizard, click **Users**.
6. Click **Remove** to remove the existing credentials, click **Add** and add the new credentials, and then click **OK**.
7. In the Service Manager console, click **Data Warehouse**.
8. In the **Data Warehouse** pane, expand **Data Warehouse**, expand **Security**, and then click **User Roles**.
9. Repeat steps 3 through 6.

To change the logon account for the Service Manager Data Access Service and Service Manager Management Configuration services

1. On the computer that hosts the Self-Service Portal, on the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, in the **Open** box, type **services.msc**, and then click **OK**.
3. In the **Services** window, in the **Services (Local)** pane, right-click **System Center Data Access Service**, and then click **Properties**.
4. In the **System Center Data Access Service Properties (Local Computer)** dialog box, click **Log On**, and then click **Browse**.
5. In the **Select User or Group** dialog box, complete these steps:

   a. Click **Locations**, in the **Locations** dialog box, click **Entire Directory**, and then click **OK**.
   b. In the **Enter the object name to select** box, type the name of the new Operational Database Account, click **Check Names**, and then click **OK**.
   c. In the **Password** and **Confirm Password** boxes, type the password for the new user, and then click **OK**.
6. Restart the Service Manager Data Access Service.
7. Right-click **System Center Management Configuration**, and then click **Properties**.
8. In the **System Center Management Configuration Properties (Local Computer)** dialog box, click **Log On**, and then click **Browse**.
9. In the **Select User or Group** dialog box, complete these steps:
   a. Click **Locations**, and in the **Locations** dialog box, click **Entire Directory**, and then click **OK**.
   b. In the **Enter the object name to select** box, type the name of the new Operational Database Account, click **Check Names**, and then click **OK**.
   c. In the **Password** and **Confirm Password** boxes, type the password for the new user, and then click **OK**.
10. Restart the Service Manager Management Configuration service.

To create a SQL Server logon

1. On the computers hosting the Service Manager and data warehouse databases, 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, complete these steps:
   a. In the **Server Type** list, select **Database Engine**.
   b. In the **Server Name** list, select the server name for your Service Manager or data warehouse databases.
   c. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
3. In the **Object Explorer** pane, expand **Security**, and then expand **Logins**.
4. Right-click **Logins**, and then click **New Login**.
5. In the **Login – New** dialog box, in the **Select a page** pane, click **General**, and then click **Search**.
6. In the **Select User or Group** dialog box, complete these steps:
   a. Click **Locations**, in the **Locations** dialog box, click **Entire Directory**, and then click **OK**.
   b. In the **Enter the object name to select** box, type the name of the new Operational Database Account, click **Check Names**, and then click **OK**.
7. In the **Select a page** pane, click **Server Roles**, and in the **Server roles** list, ensure that **sysadmin** and **public** are selected, and then click **OK**.

To change the Service Manager Self-Service Portal application pool account

1. 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** window, in the **Connections** pane, expand the name of your computer, and then click **Application Pools**.
3. In the **Application Pools** pane, right-click **SM_AppPool**, and then click **Advanced Settings**.
4. In the **Advanced Settings** dialog box, in the **Process Model** area, click **Identity**, and then click the ellipsis (**…**) button.
5. In the **Application Pool Identity** dialog box, select **Custom account**, and then click **Set**.
6. In the **Set Credentials** dialog box, in the **User name** box, type the user name for the Operational Database Account. In the **Password** and **Confirm password** boxes, type the password for the new Operational Database Account, and then click **OK**.
7. In the **Application Pool Identity** dialog box, click **OK**.
8. In the **Advanced Settings** dialog box, click **OK**.
9. Close Internet Information Services (IIS) Manager.

To change the Operational Database Account

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Security**, and then click **Run As Accounts**.
3. In the **Run As Accounts** pane, click **Operational Database Account**.
4. In the **Tasks** pane, click **Properties**.
5. In the **Operational Database Account** page, in the **User name**, **Password**, and **Domain** boxes, type the new credentials for the Operational Database Account, and then click **OK**.

How to Change the Password for the Operational Database Account

To change the log-on password for the Service Manager Data Access and Service Manager Management Configuration services

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, in the **Open** box, type **services.msc**, and then click **OK**.
3. In the **Services** window, in the **Services (Local)** pane, right-click **System Center Data Access Service**, and then click **Properties**.
4. In the **System Center Data Access Service Properties (Local Computer)** dialog box, click **Log On**.
5. Type the new password in the **Password** and **Confirm Password** text boxes, and then click **OK**.

6. Restart the Service Manager Data Access Service.
7. Right-click **System Center Management Configuration**, and then click **Properties**.
8. In the **System Center Management Configuration Properties (Local Computer)** dialog box, click **Log On**.
9. Type the new password in the **Password** and **Confirm Password** text boxes, and then click **OK**.
10. Restart the System Center Management Configuration service.

How to Change the Workflow Run As Account Credentials

During setup, you defined the account to be assigned to the Service Manager Workflow Run As account. If the password for that account changes, you must update the Workflow Run As account with the new password. If you want to change the account for the Service Manager Workflow Run As account, you must change both the Workflow Run As account and the Workflow User Role.

Use the following procedures to define a new user account for the Workflow Run As account and to update a new password for the existing account.

To change the Workflow Run As account using new credentials

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Security**, and then click **Run As Accounts**.
3. In the **Run As Accounts** pane, click **Workflow Account**.
4. In the **Tasks** pane, click **Properties**.
5. In the **Workflow Account** page, in the **User name**, **Password**, and **Domain** boxes, type the new credentials for the Workflow Run As account, and then click **OK**.
6. In the **Administration** pane, click **User Roles**.
7. In the **User Roles** pane, click **Workflows**.
8. In the **Tasks** pane, click **Properties**.
9. In the Edit User Role Wizard, click **Users**.
10. Click **Remove** to remove the existing credentials, click **Add** to add the credentials you specified in step 5, and then click **OK**.

    Important
    Failure to configure the new account for the Workflow Run As account and User Role causes Service Manager to stop functioning.

To change the password for the Workflow Run As account credentials

1. In the Service Manager console, click **Administration**.
2. In the **Administration** pane, expand **Administration**, expand **Security**, and then click

Run As Accounts.

3. In the **Run As Accounts** pane, click **Workflow Account**.
4. In the **Tasks** pane, click **Properties**.
5. In the **Workflow Account** page, in the **Password** box, type the new password for the Workflow Run As account, and then click **OK**.

How to Change the Credentials for SQL Server Analysis Services Account

If the account that is used for the SQL Server Analysis Services account changes in System Center 2012 – Service Manager, you must also change the credentials for the account. Use the following procedure to change the credentials for the SQL Server Analysis Services account.

To change the credentials for the SQL Server Analysis Services account

1. On the computer hosting SQL Server Analysis Server (SSAS), click **Start**, click **All Programs**, click **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, complete these steps:
   a. In the **Server Type** list, click **Analysis Services**.
   b. In the **Server Name** list, select the server name for your Service Manager or data warehouse databases.
   c. In the **Authentication** list, select **Windows Authentication**, and then click **Connect**.
3. In **Microsoft SQL Server Management Studios**, in the **Object Explorer** pane, expand **Databases**, expand **DWASDataBase**, expand **Data Sources**, and then double-click **DWDataMart**.
4. In **Data Source Properties – DWDataMart**, under **Security Settings**, click the ellipsis button (…) next to **ImpersonateAccount**.
5. In the **Impersonation Information** window, select **Use a specific Windows user name and password**, type the credentials for the new account, and then click **OK**.
6. Click **OK** to close **Data Source Properties – DWDataMart**, and then close Microsoft SQL Server Management Studios.

How to Change the Credentials for SQL Server Reporting Services Account

If the account that is used for the SQL Server Reporting Services account changes in System Center 2012 – Service Manager, you must change the credentials for the account. Use the following procedure to change the credentials for the SQL Server Reporting Services account.

To change the credentials for the SQL Server Reporting Services account

1. On the computer hosting SQL Server Reporting Server (SSRS), start a browser, and connect to http://<server name>/reports.
2. On the **SQL Server Reporting Services Home** page, double-click **Service Manager**, and then double-click **DWStagingAndConfig**.
3. In the **Connect using** area, click **Credentials stored securely in the report server**, type the current credentials in the **User name** and **Password** boxes, and then click **Apply**.
4. In the browser tool bar, click the **Back** button to return to the **Service Manager** page.
5. Repeat steps 2 and 3 for the remaining Service Manager data sources.

Managing Knowledge Articles in System Center 2012 - Service Manager

Knowledge articles in System Center 2012 – Service Manager can help service desk analysts and end users understand and solve problems. Because any employee can search for and view knowledge articles, create knowledge articles so that end users can help themselves resolve IT problems before new work items are opened. Service desk analysts also have to link work items to knowledge articles.

Use the procedures in this section to create and search for knowledge articles.

Managing Knowledge Article Topics

- How to Create a Knowledge Article

  Describes how to create a knowledge article.
- How to Search for a Knowledge Article

  Describes how to search for a knowledge article.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Create a Knowledge Article

You can use the following procedure to create a knowledge article in System Center 2012 – Service Manager. This procedure describes how to create a new example knowledge article to

help users obtain the latest service pack for Windows Vista. However, you can complete these steps to create any type of knowledge article.

Note

To view external content in knowledge articles, the computer on which the Service Manager console is installed must be connected to the Internet, either directly or through a proxy server.

To create a knowledge article

1. In the Service Manager console, click **Library**.
2. In the **Library** pane, expand **Knowledge**, and then click **All Knowledge Articles**.
3. In the **Tasks** pane, under **Knowledge**, click **Create Knowledge Article**.
4. In the form that appears, on the **General** tab, in the **Knowledge article information** area, follow these steps:
   a. In the **Title** box, type a title for the knowledge article. For example, type **How to obtain Windows Vista Service Pack 2**.
   b. In the description box, type a description for the article. For example, type **You can use this article to help understand this problem and to correct the problem yourself.**
5. In the **Knowledge** form, expand the **Classification** area, and then complete these steps:
   a. In the **Keywords** box, type classification keywords that you can later search, separated by semicolons. For example, type **Windows Vista; Service; Pack; 2**.
   b. In the **Knowledge Article Owner** box, browse for and then select an owner for the knowledge article. For example, select **Phil Gibbons**.
   c. In the **Category** list, select an applicable category. For example, select **Software**.
6. Expand the **External Content** area. In the **URL** box, type the web address if the information source of the article is known. For example, type **http://support.microsoft.com/kb/935791**.
7. Expand **Internal Content**. In the box, type or paste information about how the user can apply information from the **External Content** box to fix a problem that is specific to your organization. For example, type **Visit the URL to read about how to download the latest service pack for Windows Vista**.
8. Click **OK** to save the new knowledge article.

To validate that the knowledge article was created

- Verify that the new knowledge article appears in the **All Knowledge Articles** pane.

How to Search for a Knowledge Article

You can use the following procedures to search for a knowledge article by using the Service Manager console in System Center 2012 – Service Manager. If you want to link a knowledge

article to an incident or to a change request, save the incident or change request first. You can perform full-text searches when you search for knowledge articles. When you search, Service Manager queries the following fields in the knowledge search form:

- **Title**
- **Description**
- **Comments**
- **Keywords**
- **External URL**
- **Internal Content**
- **Analyst Content**

When the search is complete, Service Manager displays matches for content in the **Title**, **End-User** content, and **Analyst Content** fields. If you want to view the whole article, click **Open article to see external content**. If you type **Vista** in the search box, that exact string must exist in one of the knowledge article fields.

Note

Partial matches are not returned by a search. Therefore, when you search for a knowledge article based on a keyword, you must type the exact word. However, you can use the asterisk (*) as a wildcard character when you perform a search.

To search for a knowledge article using the Service Manager console

1. In the Service Manager console, in the search box, type a keyword or term. For example, type **Vista**.
2. Click the arrow to the right of the search box to view a list of the objects for which you want to search, and then click **Knowledge**.

The **Knowledge Search** form displays the knowledge articles that match the search term.

To search for a knowledge article when an incident or change request form is open

1. With an incident or change request form open, in the **Tasks** pane, click **Search for Knowledge Articles**.
2. In the **Knowledge Search** form, type a search term in the **Search for** box, and then click **Go**. For example, type **Vista**.

To link a knowledge article to an incident or change request

1. In the Service Manager console, in the search box, type the keyword or term for which you want to search. For example, type **Windows Vista**.
2. Click the arrow to the right of the search box to view a list of the objects for which you want to search, and then click **Knowledge**.
3. The **Knowledge Search** form displays the knowledge articles that match the search term.

4. Select the article that you want to link, and then click **Link To**.
5. In the **Select objects** dialog box, under **Filter by class**, select either **Incident** or **Change Request**.
6. Select an incident or change request, and then click **OK**.
7. Click **OK** to close the informational message.
8. In the **Knowledge Search** form, click **Close**.

Configuring and Using the System Center 2012 - Service Manager Cmdlets for Windows PowerShell

This section provides an introduction to the System Center 2012 – Service Manager cmdlets for the Windows PowerShell command-line interface.

Before you can run any command in the Windows PowerShell command-line interface in System Center 2012 – Service Manager, you must set execution policy to RemoteSigned. Before you can run data warehouse cmdlets, you must manually import the data warehouse cmdlets module.

The Service Manager cmdlets are implemented in the following two modules:

- **System.Center.Service.Manager**. This module is imported automatically every time a Service Manager Windows PowerShell session is opened.
- **Microsoft.EnterpriseManagement.Warehouse.Cmdlets**. This module must be imported manually.

Configuring and Using Service Manager Cmdlets Topics

- How to Set Execution Policy

  Describes how to set execution policy to RemoteSigned.
- Getting Started with Service Manager Cmdlets for Windows PowerShell

  Describes how to start a Windows PowerShell session in which you can run the Service Manager cmdlets and how to get help for the cmdlets.
- How to Import the Data Warehouse Cmdlet Module

  Describes how to manually import the data warehouse Windows PowerShell cmdlets.
- List of the Service Manager Cmdlets

  Provides a list of Service Manager cmdlet modules.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager

- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Set Execution Policy

Use the following procedure to set execution policy to RemoteSigned in System Center 2012 – Service Manager. This is necessary to enable the importation of the Service Manager cmdlet modules, automatically or manually.

You have to run this command only once on the computer where you intend to use Windows PowerShell cmdlets for Service Manager.

To set execution policy

1. On the computer where you want to run Windows PowerShell, click **Start**, click **All Programs**, click **Microsoft System Center 2012**, click **Service Manager**, and then click **Service Manager Shell**.
2. At the Windows PowerShell prompt, type the following command, and then press ENTER:

   ```
   Set-ExecutionPolicy -force RemoteSigned
   ```

3. Type **exit**, and then press ENTER to close the **Administrator: Windows PowerShell** window.

Getting Started with Service Manager Cmdlets for Windows PowerShell

Windows PowerShell is a Windows command-line shell that includes an interactive prompt and a scripting environment. Windows PowerShell uses cmdlets (pronounced "command-lets") to manipulate the Windows PowerShell objects. System Center 2012 – Service Manager includes many cmdlets that you can use to perform various Service Manager-related tasks without using the Service Manager console. For example, you can use the **Import-SCSMManagementPack** cmdlet to import a management pack.

The Service Manager cmdlets are delivered in two modules that are listed below. In Service Manager, these cmdlet modules are not installed in the typical path that is listed in the $env:PSModulePath variable. Therefore, if you run the `Get-Module -List` cmdlet, the Service Manager modules are not listed.

- Administrator cmdlets: The System.Center.Service.Manager module which contains the cmdlets that are needed for common administrative tasks.
- Data warehouse cmdlets: The Microsoft.EnterpriseManagement.Warehouse.Cmdlets module which contains the cmdlets that are needed for operating on the Service Manager data warehouse.

The data warehouse cmdlets operate on the data warehouse database, and you can run them on both the Service Manager management server or the data warehouse management server.

Data returned from Windows PowerShell command might contain more information than can be displayed in a default WindowsPowerShell command window. We recommend increasing the width of the command window: Right-click the title bar, click **Properties**, and in the **Layout** tab, set the **Screen Buffer Size** width to 120.

The following procedures help you to get started with Service Manager cmdlets.

To open a Service Manager Windows PowerShell session from the Service Manager console

1. In the Service Manager console, click **Administration**.
2. On the **Tasks** pane, click **Start PowerShell Session**.

The administrator cmdlet module is automatically pre-imported in this session.

To open a Service Manager WindowsPowerShell session from Windows

1. On the computer that hosts the Service Manager management server, on the taskbar, click **Start**, point to **All Programs**, and then click **Microsoft System Center**.
2. Click **Service Manager 2012**, and then click **Service Manager Shell**.

The administrator cmdlet module is automatically pre-imported in this session.

To list all Service Manager cmdlets

1. Open a Service Manager Windows PowerShell session.
2. To list the cmdlets that are included in the administrator module, in the Service Manager Windows PowerShell session, type the following, and then press ENTER:

   ```
   Get-Command -module System.Center.Service.Manager
   ```

3. To list the cmdlets that are included in the data warehouse module, in the Service Manager Windows PowerShell session, type the following, and then press ENTER:

   ```
   Get-Command –module
   Microsoft.EnterpriseManagement.Warehouse.Cmdlets
   ```

To get Help for a cmdlet

1. Open a Service Manager Windows PowerShell session.
2. You can now access the on-the-box Help, or you can use the **–online** parameter to access the most up-to-date online Help:
   - On-the-box Help: Type the following command. Replace <*cmdlet-name*> with the name of the cmdlet that you want to get help for, for example, **Import-SCSMManagementPack**:

     ```
     Get-help <cmdlet-name> -detailed
     ```

   - Online, up-to-date Help: Type the following command, and then press ENTER:

     ```
     Get-help <cmdlet-name> -online
     ```

     This command uses the **–online** parameter to access the latest online Help for a

cmdlet. It opens a web browser and displays the online Help that is available for <*cmdlet-name*>.

How to Import the Data Warehouse Cmdlet Module

To be able to use the data warehouse cmdlets in System Center 2012 – Service Manager, you must first manually import the Windows PowerShell data warehouse cmdlets module for Service Manager. You can import the data warehouse cmdlets module on the Service Manager management server, the data warehouse management server, or both.

To import the data warehouse cmdlets module

1. On a management server, open a Service Manager Windows PowerShell session. Or, on a data warehouse management server open a Windows PowerShell session.

   Ensure that the Windows PowerShell prompt is at the Service Manager installation folder.
2. At the Windows PowerShell command prompt, type the following command, and then press ENTER:

   ```
   import-module
   ".\Microsoft.EnterpriseManagement.Warehouse.Cmdlets.psd1"
   ```
3. Type **exit**, and then press ENTER to close the **Administrator: Windows PowerShell** window.

List of the Service Manager Cmdlets

System Center 2012 – Service Manager supports the following Windows PowerShell cmdlets, which are implemented in two modules: the administrator module and the data warehouse module.

Administrator Cmdlets in the System.Center.Service.Manager Module

Cmdlet	Description
Add-SCSMAllowListClass	Adds the specified classes to the Allow list of classes that is used by the Service Manager Operations Manager CI Connector during synchronization.
Export-SCSMManagementPack	Exports a management pack as a valid XML-formatted file that you can later import into Service Manager or Operations Manager.
Get-SCSMAllowList	Retrieves the Allow list of classes that is used

Cmdlet	Description
	by the Service Manager Operations Manager CI Connector during synchronization.
Get-SCSMAnnouncement	Retrieves announcements that are defined in Service Manager.
Get-SCSMChannel	Retrieves the Email Notification channels that are defined in Service Manager.
Get-SCSMClass	Retrieves a class.
Get-SCSMClassInstance	Retrieves class instance objects.
Get-SCSMCommand	
Get-SCSMConnector	Retrieves connectors that are defined in Service Manager.
Get-SCSMDCMWorkflow	Retrieves the list of desired configuration management workflows that are defined in Service Manager.
Get-SCSMDeletedItem	Retrieves items that have been marked for deletion in Service Manager.
Get-SCSMDiscovery	Retrieves discovery information from Operations Manager and from Service Manager.
Get-SCSMEmailTemplate	Retrieves Email templates that are defined in Service Manager.
Get-SCSMEmailTemplateContent	Retrieves the content of Service Manager Email templates.
Get-SCSMGroup	Retrieves groups from Operations Manager and from Service Manager.
Get-SCSMManagementGroupConnection	Retrieves all management group connections, including the IsActive state of these connections. Only one connection will have its IsActive state set to True, because only one connection can be active at any time.
Get-SCSMManagementPack	Retrieves objects that represent management packs that have been imported.
Get-SCSMObjectTemplate	Retrieves an object template.
Get-SCSMPortalCMConfiguration	Retrieves the settings for the Configuration

Cmdlet	Description
	Manager that is used for software deployments on the Service Manager Self-Service Portal.
Get-SCSMPortalContactConfiguration	Retrieves the IT Contact setting that the Service Manager Self-Service Portal is configured with.
Get-SCSMPortalDeploymentProcess	Retrieves information about software deployment processes for the Service Manager Self-Service Portal.
Get-SCSMPortalSoftwarePackage	Retrieves all the software packages that are configured for deployment in the Service Manager Self-Service Portal.
Get-SCSMQueue	Retrieves queues that are defined in Service Manager.
Get-SCSMRelationship	Retrieves information about relationship objects from Operations Manager and from Service Manager.
Get-SCSMRelationshipInstance	Retrieves the instances of relationships from Operations Manager and from Service Manager.
Get-SCSMRunAsAccount	Retrieves Run As accounts.
Get-SCSMSetting	Retrieves configuration settings of System Center Service Manager.
Get-SCSMSubscription	Retrieves subscriptions that are configured in Service Manager.
Get-SCSMTask	Retrieves tasks that are defined in Service Manager.
Get-SCSMUser	Retrieves users that are defined in Service Manager.
Get-SCSMUserRole	Retrieves user roles that are defined in Service Manager.
Get-SCSMView	Retrieves views that are defined in Service Manager.
Get-SCSMWorkflow	Retrieves configuration information for Service Manager workflows.

Cmdlet	Description
Get-SCSMWorkflowStatus	Retrieves the status of workflows in Service Manager.
Import-SCSMInstance	Imports objects and relationships from a comma-separated value (.csv) file into Service Manager.
Import-SCSMManagementPack	Imports management packs.
New-SCOrchestratorConnector	
New-SCRelationshipInstance	
New-SCSMADConnector	Creates a new Active Directory connector.
New-SCSMAlertRule	Creates an alert rule to be used with an Operations Manager 2007 alert connector in Service Manager.
New-SCSMAnnouncement	Creates a new announcement in Service Manager.
New-SCSMClassInstance	Adds a class instance to the database.
New-SCSMCMConnector	Creates a new Configuration Manager 2007 connector in Service Manager.
New-SCSMDCMWorkflow	Creates a new desired configuration management workflow in Service Manager.
New-SCSMEmailTemplate	Creates a new Email template for Service Manager.
New-SCSMManagementGroupConnection	Creates a new connection for the specified management group. The most recent management group connection that was created is the active connection that **Get-** cmdlets use by default, in which you did not specify the **ComputerName** and **Credential**, or the **SCSession** parameters.
New-SCSMManagementPack	Creates a new management pack.
New-SCSMManagementPackBundle	Bundles individual management packs and their resources, creating a new management pack bundle.
New-SCSMOMAlertConnector	Creates a new Operations Manager alert connector in Service Manager.

Cmdlet	Description
New-SCSMOMConfigurationItemConnector	Creates a new Operations Manager 2007 CI connector in Service Manager.
New-SCSMPortalDeploymentProcess	Creates a software deployment process for deploying software by using the Service Manager Self-Service Portal.
New-SCSMRunAsAccount	Creates a new Run As account.
New-SCSMSubscription	Creates a new subscription in Service Manager.
New-SCSMUserRole	Creates a new user role in Service Manager.
New-SCSMWorkflow	Creates a new workflow in Service Manager.
New-SCVMMConnector	
Protect-SCSMManagementPack	Seals a management pack, preventing it from being modified.
Remove-SCSMAllowListClass	Removes the specified classes from the Allow list of classes that are used by the Operations Manager CI Connector during synchronization in Service Manager.
Remove-SCSMAnnouncement	Removes an announcement from Service Manager.
Remove-SCSMClassInstance	Removes an instance of a configuration item object.
Remove-SCSMConnector	Removes a connector from Service Manager.
Remove-SCSMDCMWorkflow	Removes a desired configuration management workflow from Service Manager.
Remove-SCSMEmailTemplate	Removes an Email template from Service Manager.
Remove-SCSMManagementGroupConnection	Removes a management group connection.
Remove-SCSMManagementPack	Removes management packs.
Remove-SCSMPortalDeploymentProcess	Removes a software deployment process from the Service Manager Self-Service Portal.
Remove-SCSMRunAsAccount	Removes a Run As accounts.
Remove-SCSMSubscription	Removes a subscription from Service Manager.

Cmdlet	Description
Remove-SCSMUserRole	Removes a user role from Service Manager.
Remove-SCSMWorkflow	Removes a workflow from Service Manager.
Reset-SCSMAllowList	Resets the Allow list of classes that is used by the Operations Manager CI Connector in Service Manager to the default Allow list.
Restore-SCSMDeletedItem	Restores items that were previously deleted in Service Manager.
Set-SCSMChannel	Sets the properties of the email notification channel in Service Manager.
Set-SCSMManagementGroupConnection	Sets the specified connection as the active connection. The active connection is the connection that is implicitly used when you run a **Get-** cmdlet without specifying **–ComputerName** and **–Credential** or **–SCSession** parameters. Only one connection can be active at any time, and by default the active connection is the last connection that was created by using the **New-SCManagementGroupConnection** cmdlet.
Set-SCSMPortalCMConfiguration	Sets the configuration information for the Service Manager Self-Service Portal.
Set-SCSMPortalContactConfiguration	Configures the settings of information technology (IT) contacts for the end-user of the Service Manager Self-Service Portal.
Start-SCSMConnector	Starts a Service Manager connector.
Test-SCSMManagementPack	Tests the validity of a management pack.
Update-SCSMAnnouncement	Updates the properties of an announcement for Service Manager.
Update-SCSMClassInstance	Updates property values of a configuration item class instance.
Update-SCSMConnector	Updates properties of a Service Manager connector.
Update-SCSMDCMWorkflow	Updates properties of a desired configuration management workflow.

Cmdlet	Description
Update-SCSMEmailTemplate	Updates properties of an Email template.
Update-SCSMPortalDeploymentProcess	Updates the properties of software deployment processes for the Self-Service Portal.
Update-SCSMPortalSoftwarePackage	Updates the properties of software packages that are configured for deployment in the Service Manager Self-Service Portal.
Update-SCSMRunAsAccount	Updates the credentials that are associated with a Run As account.
Update-SCSMSetting	Updates the configuration settings for Service Manager.
Update-SCSMSubscription	Updates subscription properties in Service Manager.
Update-SCSMUserRole	Sets the UserRole property for a Service Manager user.
Update-SCSMWorkflow	Updates workflow properties.

Data Warehouse Cmdlets in the Microsoft.EnterpriseManagement.Warehouse.Cmdlets Module

Cmdlet	Description
Disable-SCDWJob	Disables a data warehouse job to prevent it from running.
Disable-SCDWJobSchedule	The **Disable-SCDWJobSchedule** cmdlet disables a Data Warehouse job schedule, which causes the job schedule to stop initiating jobs. If the job schedule was previously enabled, disabling the job schedule retains the job schedule settings. To modify the job schedule settings, run the **Set-SCDWJobSchedule** cmdlet.
Disable-SCDWSource	
Enable-SCDWJob	Enables a Data Warehouse job so that it can run according to its schedule.
Enable-SCDWJobSchedule	The **Enable-SCDWJobSchedule** cmdlet

Cmdlet	Description
	allows Data Warehouse administrators to enable job schedules so that jobs run according to their specified schedule. To disable the job schedule, use the **Disable-SCDWJobSchedule** cmdlet.
Enable-SCDWSource	
Get-SCDWEntity	
Get-SCDWJob	Gets the job status of all recurring jobs, including extraction, transformation, and load (ETL) jobs.
Get-SCDWJobModule	Returns detailed information for the specified job. This information includes job modules that are executed as part of the job.
Get-SCDWJobSchedule	The **Get-SCDWJobSchedule** cmdlet displays scheduling information for Data Warehouse jobs. You can use the **JobName** parameter to specify a job for which to display scheduling information. Otherwise, the **Get-SCDWJobSchedule** cmdlet displays scheduling information for all Data Warehouse jobs.
Get-SCDWModule	
Get-SCDWRetentionPeriod	The Data Warehouse grooms out rows after a predefined retention period. This cmdlet gives the retention period for a particular entity in minutes. If no entity is provided, it gives back the default retention period for all entities.
Get-SCDWSource	
Get-SCDWSourceType	
Get-SCDWWatermark	
New-SCDWSourceType	To register a source with the Data Warehouse, the Datasource Type first has to be registered with the Data Warehouse. This cmdlet helps to register a new Datasource Type by importing the suitable management pack and doing the appropriate configuration changes.

Cmdlet	Description
Register-SCDWSource	
Set-SCDWJobSchedule	Sets the schedule for a Data Warehouse job.
Set-SCDWRetentionPeriod	
Set-SCDWSource	
Set-SCDWWatermark	
Start-SCDWJob	Starts a Data Warehouse job.
Unregister-SCDWManagememtPack	
Unregister-SCDWSource	

See Also

Configuring and Using the System Center 2012 - Service Manager Cmdlets for Windows PowerShell

Managing the Data Warehouse in System Center 2012 - Service Manager

This section provides an overview of key concepts for managing the data warehouse in System Center 2012 – Service Manager. This section also contains procedures that you can use to manage the data warehouse.

Managing the Data Warehouse Topics

- About Managing the Data Warehouse

  Provides an overview of key concepts for managing the data warehouse.
- About Data Warehouse Module Deployment

  Provides an overview of data warehouse module deployment.
- Registering Source Systems to the System Center Data Warehouse

  Provides an overview about registering source systems to the data warehouse and lists procedures describing how to accomplish associated tasks.
- How to Disable a Data Warehouse Job Schedule

  Describes how to disable data warehouse job schedules.
- How to Enable Data Warehouse Job Schedules

  Describes how to enable data warehouse job schedules.
- How to View the Status of a Data Warehouse Job

  Describes how to view the job status in the data warehouse.

- How to Stop and Start a Data Warehouse Job
  Describes how to pause and resume data warehouse jobs.
- How to Schedule a Data Warehouse Job
  Describes how to schedule data warehouse jobs.
- How to View Data Warehouse Job History
  Describes how to view the data warehouse job history.
- How to Troubleshoot a Data Warehouse Job
  Describes how to troubleshoot data warehouse jobs.
- How to Configure Microsoft SharePoint for Analytics
  Describes how to configure Microsoft SharePoint Services to prepare for analytical analysis.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

About Managing the Data Warehouse

In System Center 2012 – Service Manager, there are seven data warehouse jobs that run at various times to maintain the data warehouse, as listed in the following table.

Data warehouse job	Description
MPSyncJob	This job synchronizes all the management packs from the Service Manager source. These management packs define the content of the data warehouse. This job starts to run as soon as you register the Service Manager management group, and it takes several hours to complete on its initial run. For more information, see "Register with Service Manager Data Warehouse" in the Deployment Guide for System Center 2012 – Service Manager.
DWMaintenance	This job performs data warehouse maintenance, such as indexing and updating statistics. This job will run automatically after the MPSyncJob has finished.
Entity (or Grooming)	Grooming functions typically involve activities

Data warehouse job	Description
	on the data warehouse that remove data based on a configurable time period. **Note** For this release of Service Manager, grooming functions are handled as a workflow. Settings for this job are not configurable.
Extract	This job retrieves data from the Service Manager database. This job queries the Service Manager database for the delta data from its last run and writes this new data into the DWStagingAndConfig database in the data warehouse. There are two extract jobs in Service Manager: one for the Service Manager management group and the other for the data warehouse management group.
Transform	This job takes the raw data from the staging area and does any cleansing, reformatting, and aggregation that is required to get it into the final format for reporting. This transformed data is written into the DWRepository database.
Load	This job queries the data from the DWRepository database and inserts it into the DWDatamart database. The DWDatamart is the database that is used for all end user reporting needs.

For more information about the extract, transform, and load (ETL) jobs, see the blog post Data Warehouse – Anatomy of Extract, Transform, Load (ETL).

In order to manage the data warehouse, which is primarily used by reporting, you must perform maintenance tasks on these jobs. For example, you can view their status, pause and resume, set a schedule, enable and disable schedules, and troubleshoot data warehouse jobs. You can perform all of these maintenance tasks by using Windows PowerShell cmdlets. In addition, you can perform some of these tasks through the Service Manager console.

During deployment, you registered the Service Manager management group as discussed in “Register Service Manager Management Group” in the Deployment Guide for System Center 2012 – Service Manager. As a result of that action, management pack deployment started and MPSyncJob started. You should not start or resume any data warehouse jobs until MPSyncJob has finished, as shown in the **Data Warehouse Jobs** pane in the Service Manager console.

In the procedures in the links in the following table, you can manage the data warehouse by using a combination of Windows PowerShell cmdlets and the Service Manager console, as appropriate, to perform tasks with data warehouse jobs.

Task	Reference
Enable and disable data warehouse jobs	How to Enable Data Warehouse Job Schedules
View data warehouse jobs status	How to View the Status of a Data Warehouse Job
Start and stop data warehouse jobs when you have to	How to Stop and Start a Data Warehouse Job
Schedule data warehouse jobs on a recurring basis	How to Schedule a Data Warehouse Job
Determine whether data warehouse jobs are running as expected	How to Troubleshoot a Data Warehouse Job

Job Schedule and Frequency

The schedule for a job defines when a job starts. Frequency refers to how often the job runs after it has started. Regardless of schedule and frequency, a job does not run unless the schedule for that job has been enabled. Except for the Entity (Grooming) job, each job has a default scheduled start time, which is midnight. The following table lists the scheduled start time, frequency, and default schedule setting.

Data warehouse job	Scheduled start time	Frequency	Enabled by default?
MPSyncJob	Midnight	Every hour	Yes
DWMaintenance	Midnight	Every hour	Yes
Extract	Midnight	Every 5 minutes	Yes
Transform	Midnight	Every 30 minutes	Yes
Load	Midnight	Every hour	Yes

In this release of Service Manager, grooming functions are handled as a workflow. Settings for this job are not configurable.

Windows PowerShell Cmdlets

The Service Manager Windows PowerShell module contains cmdlets that are used in this scenario to manage data warehouse functions on the server that hosts the data warehouse. You must run all Windows PowerShell cmdlets as an administrator. To view the Windows PowerShell

Help, type the **get-help** command, followed by the name of the cmdlet for which you want help. For example, type `get-help Set-SCDWJobSchedule`. The following cmdlets are used in this scenario:

- **Get-SCDWJobSchedule**—Displays the schedule for a data warehouse job.
- **Get-SCDWJob**—Displays status for all recurring Service Manager data warehouse jobs.
- **Get-SCDWMgmtGroup**—Shows details for a management group that is registered with the data warehouse.
- **Remove-SCDWMgmtGroup**—Removes a management group from the data warehouse.
- **Set-SCDWJobSchedule**—Sets the schedule for data warehouse jobs.
- **Enable-SCDWJobSchedule**—Enables a data warehouse job schedule.
- **Disable-SCDWJobSchedule**—Disables a data warehouse job schedule. Job schedules are disabled by default.

For information about how to run Service Manager Windows PowerShell cmdlets, see Getting Started with Service Manager Cmdlets for Windows PowerShell.

Getting Started with Data Warehouse Jobs

When you register with the Service Manager data warehouse (see "Register with Service Manager Data Warehouse" in the Deployment Guide for System Center 2012 – Service Manager, the MPSyncJob starts running. This job can take several hours to complete its initial run. When this job is complete, you can see two extract jobs listed in the Data Warehouse Jobs pane. One extract job is listed as **Extract_<data warehouse management group name>**, and the other extract job is listed as **Extract_<Service Manager management group name>**. When both of these extract jobs appear, you know that the initial run of the MPSyncJob is complete and that you can now proceed with the subsequent maintenance tasks.

See Also

About_Data_Warehouse_Jobs

About Data Warehouse Module Deployment

Data warehouse module deployment in System Center 2012 – Service Manager starts when a Service Manager management server is registered to a data warehouse management server. The following sections describe module parts, functions, and schedule.

Management Pack Synchronization

Management pack synchronization is the process by which the data warehouse discovers what classes and relationships exist in source systems. This process is also referred to as MPSync. For every management pack that defines a class or relationship, the data warehouse creates extract job modules to retrieve the data for that class or relationship from the corresponding source. Such management packs and their associated jobs are synchronized between the systems.

Only sealed management packs, and their corresponding data, are synchronized into the data warehouse. If you alter a management pack, you must increase the version number and you cannot introduce any changes that might cause errors; otherwise, the management pack will fail to import. For example, you cannot remove classes, remove properties, or remove relationships. Similarly, you cannot change data types in unsupported ways. For example, you cannot modify a string property to become a numeric property.

By default, the MPSync Orchestration job runs every 30 minutes.

It is possible that multiple sources may refer to the same management pack. The version in the source system must be the same or higher version than that in the data warehouse, otherwise registration will fail.

It is possible to remove management packs from the data warehouse. However, keep the following points in mind:

1. Removing management packs does not delete the data from the data warehouse as it does in the Service Manager database; instead, the database view that users are granted access to is dropped.
2. If you reimport a management pack after you have removed the corresponding management pack, the historical data is exposed once again.

> **Note**
> Only sealed management packs are synchronized from Service Manager to the data warehouse. An exception to this is list items, also known as enumerations. Groups or queues are synchronized to the data warehouse, regardless of whether they are in a sealed or unsealed management pack. For more information about how to seal a management pack, see the blog post Sealing Management Packs.

Management packs that are imported from Service Manager are Service Manager–specific and data warehouse specific. The Service Manager management packs provide awareness of what the Service Manager database is structured like, and the data warehouse management packs drive the structure and processes of the data warehouse databases.

Report Deployment

The management pack synchronization process imports management packs from Service Manager, and it defines how those management packs shape the structure, move the data, and copy reports for the data warehouse and reporting. After those management packs are synchronized between Service Manager and the data warehouse, the data is retrieved and reports are deployed for user consumption.

Sequentially, report deployment occurs in the following process:

1. After all identified management packs are synchronized with data warehouse, management pack synchronization triggers the report deployment workflow.
2. Because the DWStagingandConfig database is the final destination of the management packs that have been synchronized, the deployment workflow queries the DWStagingandConfig database for any new or changed reports to deploy or any reports to remove.

3. The deployment workflow then publishes any new or updated reports to the SQL Server Reporting Services (SSRS) server through the SSRS web services.
4. SSRS stores the reports and appropriate metadata.
5. Schema deployment workflow is triggered by management pack synchronization.
6. Once again, information that causes schema changes is retrieved from the DWStagingandConfig database based on the newly synchronized management packs that are causing the changes.
7. Schema changes are deployed to the DWRepository database.
8. Any necessary changes to extract, transform, and load (ETL) modules are made to the DWStagingandConfig database.

Management packs that contain onlyService Manager–specific information do not cause the deployment activities to execute. They are only be triggered for new data warehouse and reporting-specific elements.

Understanding the ETL Processes

After the data warehouse schema and reports are deployed, the DWDataMart database is populated with actual data for reporting purposes. This is done by the ETL processes. These three processes each serve their own specific purpose:

- **Extract** is designed specifically for processing large volumes of data from multiple sources, and it allows for moving data into an area that is built for manipulating the data.
- **Transform** is designed for optimization of complex logic and integration operations. This process is where most of the ETL work occurs.
- **Load** is designed for transferring the data that has already been processed into its target destination in a bulk manner.

One of the main reasons for having three different databases is so that you can optimize your hardware environment more easily. In high-volume environments, the DWStagingandConfig and DWRepository databases must be on computer hardware that is optimized for read/write I/O. However, the computer hardware hosting the DWDatamart database must be optimized for read I/O. With that difference in mind, you can separate the DWDatamart to a different server or drive from the DWStagingandConfig and DWRepository databases. However, the DWStagingandConfig and DWRepository databases must remain on the same server.

At a high level, ETL occurs in the processes described in the following sections. If you plan on authoring management packs that are used for custom reporting, you will probably need to know more about these processes in depth. For more information about ETL processes, see the Authoring Guide for System Center 2012 - Service Manager.

Extract

The extract process starts on a scheduled interval. Extract is the process that retrieves raw data from your online transaction processing system (OLTP) store, which in this case is the Service Manager database.

1. The extract process queries Service Manager for the delta data that has accumulated since the last time the extract process ran.

2. The new data is written into the DWStagingandConfig database in the same basic form as it is in the Service Manager database.

Transform

The transform process starts on a scheduled interval. Transform is the process that moves the raw data from the DWStagingandConfig database. It also does any cleansing, reformatting, and aggregation that is required to alter the raw data into the final format for reporting. This transformed data is written into the DWRepository database.

Load

The load process starts on a scheduled interval. The load process queries for the data from the DWRepository database. The transformed data from DWRepository is inserted into the DWDatamart database. The DWDatamart is the database that is used for all end-user reporting needs.

About Reimporting Previously Removed Management Packs

During development and testing of management packs that contain reports that access data warehouse information, you might need to remove the management packs and then reimport them later. However, after a management pack is uninstalled from the data warehouse, if the new management pack contains the same dimension, fact, or cube name with a schema that is different from the original, you must delete the dimension or fact table from the DWRepository and DWDataMart databases manually and also delete any referencing cube from the SQL Server Analysis Services (SSAS) database.

In addition, if a dimension or fact is already referenced by an existing data cube, you must also delete the management pack that contains the data cube and the data cube itself before uninstalling the new management pack. Because System Center 2012 – Service Manager does not remove the dimension or fact table from the DataSourceView and because dimensions are not removed from SSAS database, you must manually delete information that a data cube references. In this situation, you should use SQL Server Management Studio to remove any custom data cube that you created with the management pack from the DWASDatabase before you reregister or reinstall an updated management pack.

In general, you should avoid having the same dimension, fact, and cube name in differing schemas. Service Manager does not support this condition.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

Registering Source Systems to the System Center Data Warehouse

The data warehouse in System Center 2012 – Service Manager retrieves data from one or more data sources. These data sources are the transactional processing systems that produce and

govern data that you will eventually want to measure and analyze. For example, incidents and change requests are created and managed in Service Manager, software updates and power policies are managed in Configuration Manager, and other systems produce and govern other data sets.

Registering the data warehouse creates a relationship between the data warehouse server and the source system so that information can flow between them. In Service Manager, you can register to Service Manager, Operations Manager, and Configuration Manager directly. You can also use the updated software development kit (SDK) layer on top of the data warehouse, which enables you to push data into the data warehouse directly from other sources. For example, you might want to push data from your Human Resources computer system in the data warehouse.

Registering Source Systems Topics

- How to Register the System Center Data Warehouse to Operations Manager

  Describes how to register with Operations Manager and then validate the registration.
- How to Register Configuration Manager With the System Center Data Warehouse to

  Describes how to register with Configuration Manager and then validate the registration.
- How to Register the System Center Data Warehouse to a Service Manager Source

  Describes how to register with another Service Manager data source and then validate the registration.
- How to Manage Data Import Jobs for Operations Manager and Configuration Manager

  Describes how to manage data import jobs and change a job schedule.
- Troubleshooting System Center Data Warehouse Errors

  Describes steps you can take to troubleshoot System Center data warehouse errors.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Register the System Center Data Warehouse to Operations Manager

You can use the following procedures in System Center 2012 – Service Manager to register the System Center Data Warehouse to Operations Manager and then validate the registration.

To register the data warehouse to Operations Manager

1. By using an account that is a member of the Service Manager and data warehouse management administrators group, log on to the computer that hosts the Service Manager console.
2. In the Service Manager console, select **Data Warehouse**.

3. In the **Administration** pane, expand **Data Warehouse**, and then select **Data Sources**.
4. In the **Tasks** list, click **Register data source**.
5. In the Register Data Source Wizard, on the **Before You Begin** page, click **Next**.
6. On the **Data Source Type** page, select **Operations Manager**.
7. Under **Specify a Root Management Server** area, type the following information:
   a. For **Root Management server name**, type the server name.
   b. For **Operational database server**, type the database server name.
   c. For **Database name**, type the name of the database.
8. Click **Next**.
9. On the **Credentials** page, you can accept the default entry in the **Run as account** list, and then click **Next**, or you can enter credentials from a user or group of your choice.

   Important
   The account that you specify will be assigned administrative credentials on the Service Manager management server and granted Read permission on the Service Manager database. You can specify different credentials from other Service Manager management groups when you are registering with the data warehouse.
10. On the **Summary** page, you can review the settings that you have chosen. Click **Finish**.
11. On the **Result** page, when **Data source registration complete.** appears, click **Finish**.

To validate theOperations Manager registration process

- In the **Data Sources** view, the new data source appears in the list of data sources, with the data source type of **Operations Manager**. You might have to refresh your view to see the new data source.

See Also

Registering Source Systems to the System Center Data Warehouse

How to Register Configuration Manager With the System Center Data Warehouse to

You can use the following steps in System Center 2012 – Service Manager to register Configuration Manager with the System Center Data Warehouse and then validate the registration.

To register Configuration Manager with the data warehouse

1. By using an account that is a member of the Service Manager and data warehouse management administrators group, log on to the computer that hosts the Service Manager console.
2. In the Service Manager console, select **Data Warehouse**.

3. In the **Administration** pane, expand **Data Warehouse**, and then select **Data Sources**.
4. In the **Tasks** list, click **Register data source**.
5. In the Register Data Source Wizard, on the **Before You Begin** page, click **Next**.
6. On the **Data Source Type** page, select **Configuration Manager**.
7. Under **Specify a Central Site Server**, type the following information:
   a. For **Central Site server name**, type the site server name.
   b. For **Database name**, type the name of the database.
8. Click **Next**.
9. On the **Credentials** page, you can accept the default entry in the **Run as account** list, and then click **Next**, or you can enter credentials from a user or group of your choice.

   Important
   The account that you specify will be assigned administrative credentials on the Service Manager management server and granted Read permission on the Service Manager database. You can specify different credentials from other Service Manager management groups when you are registering with the data warehouse.
10. On the **Data Selection** page, choose the domains to extract, and then click **Next**. For example, select **System Center Configuration Manager Connector Configuration** and **System Center Configuration Manager Power Management Connector**.
11. On the **Summary** page, you can review the settings that you have chosen. Click **Finish**.
12. On the **Result** page, when **Data source registration complete** appears, click **Finish**.

To validate the Configuration Manager registration process

- In the **Data Sources** view, the new data source appears in the list of data sources, with the data source type of **Configuration Manager**. You might have to refresh your view to see the new data source.

See Also

Registering Source Systems to the System Center Data Warehouse

How to Register the System Center Data Warehouse to a Service Manager Source

You can use the following procedures in System Center 2012 – Service Manager to register the System Center Data Warehouse with a Service Manager management group and then validate the registration. This makes it possible to host multiple Service Manager management groups in a single data warehouse.

To register the data warehouse with another Service Manager management group

1. By using an account that is a member of the Service Manager and data warehouse management administrators group, log on to the computer that hosts the Service

Manager console.

2. In the Service Manager console, select **Data Warehouse**.
3. In the **Administration** pane, expand **Data Warehouse**, and then select **Data Sources**.
4. In the **Tasks** list, click **Register data source**.
5. In the Register Data Source Wizard, on the **Before You Begin** page, click **Next**.
6. On the **Data Source Type** page, select **Service Manager**.
7. Under **Specify a Service Manager Server**, type the following information:
   a. For **Service Manager server name**, type the server name.
8. Click **Next**.
9. On the **Credentials** page, you can accept the default entry in the **Run as account** list, and then click **Next**, or you can enter credentials from a user or group of your choice.

   Important
   The account that you specify will be assigned administrative credentials on the Service Manager management server and granted Read permission on the Service Manager database. You can specify different credentials from other Service Manager management groups when registering with the data warehouse.
10. On the **Summary** page, you can review the settings that you have chosen. Click **Finish**.
11. On the **Result** page, when **Data source registration complete.** appears, click **Finish**.

To validate the Service Manager registration process

- In the **Data Sources** view, the new data source appears in the list of data sources, with the data source type of **Service Manager**. You might have to refresh your view to see the new data source.

See Also

Registering Source Systems to the System Center Data Warehouse

How to Manage Data Import Jobs for Operations Manager and Configuration Manager

You can use the following procedure to manage data warehouse data import jobs in System Center 2012 – Service Manager. Data import jobs are like other data warehouse jobs, and you can manage them with the Service Manager console and also with Windows PowerShell cmdlets. Methods of management include:

- Revising the processing schedule to hourly, daily, or weekly
- Suspending a job
- Resuming a suspended, or Not Started, job

To manage data import jobs and change a job schedule

1. In the Service Manager console, click **Data Warehouse**, expand **Data Warehouse**, and then click **Data Warehouse Jobs**.
2. In the **Data Warehouse Jobs** pane, select a job name, and then under **Tasks**, click **Properties**.
3. In the job properties dialog box that appears, you can view the current schedule. You can change the schedule to one of your choice. For example, change the schedule to **Daily** and run the job at **1:00 AM**, and then click **OK**.
4. You can optionally **Suspend** jobs, and you can **Resume** any that are suspended or Not Started.

See Also

Registering Source Systems to the System Center Data Warehouse

Troubleshooting System Center Data Warehouse Errors

This section describes steps you can take to troubleshoot System Center data warehouse errors in System Center 2012 – Service Manager.

Using the Operations Manager event log on the Data Warehouse server to troubleshoot errors

Service Manager event logs are found in the Operations Manager event log. Evaluating events in the log is useful because most errors from the data warehouse are found in this event log. Events in the log are from two different sources: Deployment and Data Warehouse.

Events with a source of **Deployment** are usually generated during management pack deployment, which includes report deployment or assembling the data warehouse, for example, by creating outriggers, dimensions, and fact tables. Errors in the event log usually include instructions about how to recover from the errors. For example, you might read instructions suggesting that you stop and then restart the Service Manager services. The three services on a data warehouse management server are:

- System Center Data Access Service
- System Center Management
- System Center Management Configuration

When you start and stop Service Manager services, you must stop and start all three services.

After the data warehouse is deployed, events are more likely to have a source of **Data Warehouse**. These events are created by jobs within the normal course of operations like extract, transform, and load (ETL) jobs; the MPSync job; and the DWMaintenance job.

Using the Service Manager console to troubleshoot errors

In the Service Manager console, click **Data Warehouse Jobs** and you will see ETL job and MPSync job status. If your deployment was successful and your data warehouse is correctly registered to at least one Service Manager management group, you see at least five jobs. Every job should have the status **Running** or **Not Started**.

If you see a job status listed as **Failed**, you can select the job, and then in the **Tasks** pane, click **Modules** to find out which job module has failed. Then, you can examine the Operations Manager event log on the data warehouse server to determine why the module failed.

In the **Data Warehouse** workspace, you can click **Management Packs** in the left pane. That is where you can view all the management packs in the data warehouse and the status of their deployment. When you import a management pack toService Manager, the MPSync job synchronizes it to the data warehouse, where the MPSync job derives its name from management pack synchronization. When you get the list of management packs in the data warehouse, you can find out if your management pack has been deployed successfully or not.

If your management pack has defined data warehouse-specific elements, such as outriggers, dimensions, fact tables, or reports, that management pack must be successfully deployed before the new tables and reports will be ready to use.

Using Windows PowerShell to troubleshoot errors

The Windows PowerShell cmdlets in the following table provide detailed information about the data warehouse jobs.

Command	Description
Get-SCDWMgmtGroup	This command tells you which sources are currently registered with the data warehouse. You should expect to see at least two different DataSourceName values.
Get-SCDWJob	This command lists the data warehouse job status of the current batch. Using the command, you can check whether the jobs are enabled or not, which jobs are running, and when they started. When the MPSync or DWMaintenance jobs start, they disable all of the ETL jobs. You will see the **Is Enabled** column set to **False** for each of the ETL jobs. This means that even if the ETL job status shows it is running, it actually is not running. When the MPSync or DWMaintenance job completes, the ETL jobs are automatically enabled and resume processing. Jobs normally have the **Not Started** status, unless the previous batch has completed. If you prefer, you can use the **Get-SCDWJob** command to view the last few batches of a specific job.

Command	Description
Get-SCDWJob –JobName <Specific job name> -NumberOfBatches <number>	Use this command to see the latest job, specified by <Specific job name>, completed, when it started, and when it ended. You can calculate how long it ran and what the next batch ID and status is. The job batch ID is always incremental.
Get-SCDWJobModule	This command provides detailed information about the specific modules within the job. This is very useful when you see job failures and you want to find out what caused the failure.

Troubleshooting Common Data Warehouse Issues

This list is not exhaustive, but it covers most of the common problems that you are likely to encounter.

Reports are not deployed after registering the data warehouse

Symptoms

When you open the Service Manager console, a dialog box appears indicating that the Reporting Service is unavailable. Another symptom is that the **Reporting** workspace button appears in the Service Manager console; however, there are no reports displayed in the workspace. Another symptom is that no reports have been deployed to the Reporting Services server.

Other aspects of the data warehouse deployment might appear to have gone smoothly. For example, in the Service Manager console, when you click **Data Warehouse**, and then click **Data Warehouse Jobs**, you see two extract jobs, a transform and load job, and an MPSync job.

Troubleshooting Steps

To troubleshoot this problem, complete the following steps.

Step 1: Check the deployment status of your management packs:

1. In the Service Manager console, click **Data Warehouse**.
2. Click **Management Packs**, and in the search **Filter** box, type **report**. This filters results to report-related management packs.
3. Check the deployment status (last column) of the following management packs. None of the management packs should have a status of **Failed**.
   - ServiceManager.ActivityManagement.Report.Library
   - ServiceManager.ProblemManagement.Report.Library
   - ServiceManager.IncidentManagement.Report.Libraryxxx
   - ServiceManager.ConfigurationManagement.Report.Library
   - ServiceManager.ChangeManagement.Report.Library

Step 2: Check the event log for error messages that mention the assembly Microsoft.EnterpriseManagement.Reporting.Code.dll file.

If any of the above five management packs failed deployment:

1. On the data warehouse management server, open the Operations Manager event log.
2. Filter the events with **Event Sources** as **Deployment** and **Event Level** as **Error**.
3. If there are error messages in the event log that indicate **cannot load Assembly Microsoft.EnterpriseManagement.Reporting.Code.dll**, review the following items:
   a. Your installation of SQL Server Reporting Services (SSRS) may be on a different server than the data warehouse management server. If so, refer to the instructions in the Deployment Guide for System Center 2012 – Service Manager and copy the assembly to the SSRS server, and then add access permission to it.
   b. If your SSRS installation is on the same server as the data warehouse management server, restart the SSRS service.
4. Restart SSRS:
   a. Log on to the server where SSRS is installed.
   b. Click **Start**, **All Programs**, **Microsoft SQL Server 2008** (or **Microsoft SQL Server 2008 R2**), **Configuration Tools**, and then click **Reporting Services Configuration Manager**.
   c. In the **Reporting Services Configuration Connection** window, click **Connect**.
   d. In the **Reporting Server Status** window, click **Stop**, and then click **Start**.
   e. Click **Exit**.

Step 3: Redeploy any failed report management packs:

1. In the Service Manager console, click **Data Warehouse**.
2. Click **Management Packs**, and then in the search filter, type **report**.
3. For each of the management packs listed in step 1, in the **Tasks Pane**, click **Restart Deployment**.

   Note
   If the deployment status of a management pack is listed as **Completed**, the **Restart Deployment** option is unavailable.

After the deployment status of the report management packs has updated from **Failed** to **Completed**, open the Service Manager console. Reports should display in the **Reporting** workspace. You may have to restart the Service Manager console to view the reports because the console caches the list of reports.

Jobs fail after importing a custom management pack

Symptom

One or more data warehouse jobs start failing after importing a custom management pack and synchronizing it to the data warehouse.

Troubleshooting Steps

To troubleshoot this problem, complete the following steps:

1. Check the event log to ensure that the root cause is the custom management pack:

   a. On data warehouse management server, open the Operations Manager event log.
   b. Find the event that is related to the job failure.
   c. Determine if the failure is related to the custom management pack you imported.
2. If the failure is related to the custom management pack, you should remove it and let the rest of the data warehouse operate as usual. You can fix the management pack and reimport it later:
   a. Uninstall the custom management pack using the Service Manager console.
   b. Run the MP Sync job.
   c. Verify that the custom management pack is listed in **Data Warehouse** under **Management Packs**.
   d. After the MP Sync job is completed, resume the failed job either from the Service Manager console or with a Windows PowerShell cmdlet.
3. Fix and reimport the custom management pack:
   a. Remove the custom management pack and recover from the failure using step 2, shown previously.
   b. Fix the custom management pack.
   c. Import the fixed custom management pack into Service Manager, and then run the MP Sync job to sync it to the data warehouse.

Data warehouse is not receiving new data, or jobs seem to take too long to complete

Symptom

You do not see data or new data in any of your reports. Another symptom is that ETL jobs are taking too long to run and the jobs do not show a status of **Not Started**.

Troubleshooting Steps

To troubleshoot this problem, complete the following steps:

1. Use the Windows PowerShell cmdlet **Get-SCDWJob** to determine if all ETL jobs are enabled. Start Windows PowerShell, and then type **Get-SCDWJob**.
2. If the ETL jobs are disabled and either the MPSyncJob or DWMaintenance jobs are running, you will haveto wait awhile to get the job status again because these two background jobs disable the ETL jobs. However, if the two jobs are listed as **Not Started** and the ETL jobs are disabled, you can use the **Enable-SCDWJob** cmdlet to enable each of them, for example:

   ```
   Enable-SCDWJob -JobName Transform.Common
   ```

3. If the MPSync and DWMaintenance ETL jobs are all enabled and running but their individual batch ID has not changed for a long time, or if you use the **Get-SCDWJobModule** cmdlet for specific jobs and you do not see that any module is actually running, check the event log and see if there are any error messages. Sometimes the error message might be many days old and you might need to review many days-worth of events.
4. Check if the three services—System Center Data Access Service, System Center Management, and System Center Management Configuration—on the data warehouse management server are actually running. On the data warehouse management server, click **Start**, click **Run**, and then type **Services.msc**. In **Services** verify that the following services

are running: System Center Data Access Service, System Center Management, and System Center Management Configuration.

If any of the services are not running, restart all three services. In addition, if all services are actually running, events from the Event Source Data Warehouse and OpsMgr SDK Service are sent to the Operations Manager event log. You can use this information as another source to verify whether all the services are running. If you do not see events from the Event Source Data Warehouse and OpsMgr SDK Service for a long time, you should restart all three services.

Custom data warehouse extensions do not appear in the data warehouse

Symptom

After importing your management pack, which defines some dimensions or fact tables to Service Manager, the MPSync job has run several times, but you still do not see your dimension or fact tables in the DataMart.

Troubleshooting Steps

Ensure that your management pack is sealed. The MPSync Job can import only sealed management packs from Service Manager into the data warehouse. If you have not sealed your management pack, seal it, and then import it using the Service Manager.

Ensure that your management pack is synced to the data warehouse by completing the following steps:

1. Open the Service Manager console.
2. Click **Data Warehouse**.
3. Click **Management Packs**, and then locate your management pack in the list of management packs. To do this, use the search feature by typing your management pack name in the search box. If you do not see your management pack:
   a. It might have failed to import into the data warehouse management server. Go to the data warehouse management server, open the Operations Manager event log and then filter the events with **Event Sources** as **OpsMgr SDK Service**.
   b. The MPSync job may not have run yet. It runs on a recurring schedule, which is, by default, once every hour. You can modify the schedule with Windows PowerShell. Tto speed up management pack synchronization, after you import your management pack you can manually resume the MPSync job, either from the Service Manager console or by using Windows PowerShell.

Check the deployment status of your management pack:

1. Open the Service Manager console.
2. Click **Data Warehouse**.
3. Click **Management Packs**, and then find your management pack in the list of management packs. To do this you can search for your management pack name.
4. Check the deployment status of your management pack. If the deployment status is **Failed**:
   a. On the data warehouse management server, open the Operations Manager event log, and then filter the events with **Event Sources** as **Deployment**.

b. If there is an error message, the message usually indicates what went wrong. If after you make any needed fixes to the management pack and the error still occurs, you can uninstall this management pack using the Service Manager console. After the MPSync job runs, the management pack is uninstalled from data warehouse management server.

Management packs are stuck in Pending Association status after registering to the data warehouse

Symptom

Some management packs remain in **Pending Association** status several hours after registering Service Manager with the data warehouse and several (up to four or more) hours have passed. You can determine the time elapsed by opening the **smcons** and navigating to **Data Warehouse**, **Data Warehouse Jobs**, **MPSync Job**, and then clicking **Details** from the **Tasks** pane.

Troubleshooting Steps

To troubleshoot this problem, complete the following steps:

1. View the **Details** of the MPSync job. Review each batch ID for the problem management pack in the **MPSyncJob** dialog box. In the **MP Sync Job** dialog box, click the **Management Pack** column name to sort the list according to management pack name. Find any management packs with **Pending Association** status. In the list of management packs, check to see if, in the later batch, the management pack status is listed as **Associated**, for example:
   - For Batch ID 136, Management Pack Microsoft.SystemCenter.ConfigurationManager is Pending Association.
   - For Batch ID 207, Management Pack Microsoft.SystemCenter.ConfigurationManager is Associated.

   This indicates the management pack is associated properly in batch 207, even though it ran into an error in batch 136. Because it recovered in batch 207, the management pack is correctly associated and the synchronization completed successfully.
2. If in the **MP Sync Job** dialog box, the Pending Association status for a management pack repeats for every batch, you will have to troubleshoot further to determine the reason why the management pack fails to associate. You should start by looking for deployment failures in other management packs that your management pack depends on.

   In the Service Manager console, click **Data Warehouse**, click **Management Packs**, and then click the **Deployment Status** column heading. If you see any management pack with a deployment status of **Failed** or **Not Started**, this is usually due to a management pack dependency. Because management packs can depend on others, any failure can cause other management packs to fail deployment. Any impacted management pack has the **Not Started** status.
3. Find the deployment failures in the event log. Open the Operations Manager Event log on the data warehouse, filter the event log to the events where the Event Source is **Deployment** and Event Level is **Warning** or **Error**.
4. If there is an error message similar to the following message, you will have to unregister the data warehouse from Service Manager, reinstall the data warehouse, and then reregister the Service Manager management server to the data warehouse management server:

```
Deployment Execution Infrastructure has retried the maximum
number of times and is giving up on this execution step.
MP Element ID:
DerivedManagementPack.SystemDerivedMp.ServiceManager.ActivityMan
agement.Library.Datawarehouse
MP name: ServiceManager.ActivityManagement.Library.Datawarehouse
MP version: 7.0.5826.0
Operation: Install
Error message:  Cannot find resource with ID
TransformActivityStatusResource
```

ETL jobs fail due to login credentials problems

Symptom

Some or all ETL jobs have failed. The Operations Manager event log on the data warehouse management server indicates that the ETL job failure is related to a login user failure.

Troubleshooting Steps

To troubleshoot this problem, check if the password for each Run As account has changed or expired. You can update the account using the following steps:

1. Navigate to **Data Warehouse**, **Security**, **Run As Accounts**, and then click the related run as account. Click **Properties** in the **Tasks** pane, update the **Password** field in the window, and then click **OK**.
2. If this Run As account is an Operational System Account, you also have to update the services that are running under the account:
   a. On the data warehouse management server, click **Start**, click **Run**, and then type **Services.msc**.
   b. In **Services**, update the passwords for the services that run under the account, for example, System Center Data Access Service and System Center Management Configuration.
   c. Restart the services.

   Note
   The MP Sync job and Extract jobs can use a different Run As account other than Operational System Account. This Run As account is created when Service Manager is registered to a data warehouse.

It is easy to update the password if it is expired. However it is more difficult to update the system if you change the Run As account. We do not recommend that you modify Run As accounts.

If the job failure is not related to the password, make sure that the Run As account for the failed job can be used to connect to the target database. For example, ensure that the Extract job Run As account can be used to connect to the Service Manager database. If not, make sure that the Structured Query Language (SQL) service that is hosting the database is running.

See Also

Registering Source Systems to the System Center Data Warehouse

How to Disable a Data Warehouse Job Schedule

You can use the following procedure to disable the schedule for the extract, transform, and load (ETL) jobs; however, you can use this procedure to disable the schedule for any data warehouse job. In this release of Service Manager (System Center 2012 – Service Manager), you can disable the schedules only by using Windows PowerShell cmdlets.

Note

For information about how to run Service Manager Windows PowerShell cmdlets, see Getting Started with Service Manager Cmdlets for Windows PowerShell.

To disable a schedule for a data warehouse job by using Windows PowerShell cmdlets

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. At the Windows PowerShell prompt, type the following commands, and press ENTER after each command:

```
Disable-SCDWJobSchedule -JobName Extract_<data warehouse
management group name>
Disable-SCDWJobSchedule -JobName Extract_<Service Manager
management group name>
Disable-SCDWJobSchedule -JobName Transform.Common
Disable-SCDWJobSchedule -JobName Load.Common
```

3. Type **exit**, and then press ENTER.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to Enable Data Warehouse Job Schedules

Use the following procedure to enable the schedule for the ETL jobs as needed; you can use this procedure to enable the schedule for any of the data warehouse jobs. By default, the schedules for the extract, transform, and load (ETL) jobs are enabled. In this release of Service Manager (System Center 2012 – Service Manager), you can enable the schedules only by using Windows PowerShell.

To enable a schedule for a data warehouse job by using a Windows PowerShell cmdlet

1. On the computer that hosts the data warehouse management server, click **Start**, point to

All Programs, click **Microsoft System Center**, click **Service Manager 2012**, and click **Service Manager Shell**.

2. At the Windows PowerShell prompt, type the following commands, and then press ENTER after each command:

```
Enable-SCDWJobSchedule -JobName Extract_<data warehouse
management group name>
Enable-SCDWJobSchedule -JobName Extract_<Service Manager
management group name>
Enable-SCDWJobSchedule -JobName Transform.Common
Enable-SCDWJobSchedule -JobName Load.Common
```

3. Type **exit**, and then press ENTER.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to View the Status of a Data Warehouse Job

You can use the following procedures to view the status of a data warehouse job in System Center 2012 – Service Manager to determine whether a job is running, stopped, or failed.

Note

For information about running Service Manager Windows PowerShell cmdlets, see Getting Started with the Service Manager Cmdlets in the Administrator's Guide for System Center 2012 - Service Manager.

To view the status of a data warehouse job by using the Service Manager console

1. In the Service Manager console, click **Data Warehouse**.
2. In the **Data Warehouse** pane, expand **Data Warehouse**, and then click **Data Warehouse Jobs**.
3. In the **Data Warehouse Jobs** pane, review the list of jobs to view their status.

To view the status of a data warehouse job by using a Windows PowerShell cmdlet

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. Type the following command, and then press ENTER.

```
Get-SCDWJob
```

3. Review the list of jobs to view their status.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to Stop and Start a Data Warehouse Job

You can stop and start data warehouse jobs that are running in System Center 2012 – Service Manager. For example, you might have to stop all of the data warehouse jobs that are running to ensure that a security update to the data warehouse management server does not interfere with any jobs that might run. After the server has been updated and restarted, you resume all the data warehouse jobs. You can stop and then start jobs by using the Service Manager console or by using Windows PowerShell cmdlets. In this example, only the extract, transform, and load (ETL) jobs are running.

Note

For information about using the Service Manager Windows PowerShell cmdlets, see Getting Started with Service Manager Cmdlets for Windows PowerShell.

To stop and start data warehouse jobs using the Service Manager console

1. In the Service Manager console, click **Data Warehouse**.
2. Expand **Data Warehouse**, and then click **Data Warehouse Jobs**.
3. In the **Data Warehouse Jobs** pane, select a job that is running, and then click **Suspend** in the **Tasks** list.
4. Repeat the previous step for each data warehouse job.
5. To resume each job, select a job that is stopped in the **Data Warehouse Jobs** pane, and then click **Resume** in the **Tasks** list.

To stop all data warehouse jobs using Windows PowerShell cmdlets

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. At the Windows PowerShell prompt, type the following commands, and then press ENTER after each command:

```
Stop-SCDWJob-JobName Extract_<data warehouse management group name>
Stop-SCDWJob -JobName Extract_<Service Manager management group name>
Stop-SCDWJob -JobName Transform.Common
Stop-SCDWJob -JobName Load.Common
```

3. Type **exit**, and then press ENTER.

To start all data warehouse jobs using Windows PowerShell cmdlets

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. At the Windows PowerShell prompt, type the following commands, and then press ENTER after each command:

```
Start-SCDWJob –JobName Extract_<data warehouse management group name>
Start-SCDWJob –JobName Extract_<Service Manager management group name>
Start-SCDWJob –JobName Transform.Common
Start-SCDWJob –JobName Load.Common
```

3. Type **exit**, and then press ENTER.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to Schedule a Data Warehouse Job

You can use the following procedure to schedule a data warehouse job in System Center 2012 – Service Manager.

You could use this procedure in a scenario where a schedule for the data warehouse jobs has been defined in Service Manager. You want to change the schedule for the data warehouse jobs to define standard maintenance windows for the Service Manager database and for the data warehouse. Use the **Set-SCDWJobSchedule** cmdlet to schedule the data warehouse jobs. The **Set-SCDWJobSchedule –ScheduleType Weekly** cmdlet and parameter combination allows jobs to run only on the days you specify. For example, the following commands define a daily or weekly schedule:

```
Set-SCDWJobSchedule -JobName Transform.Common –ScheduleType Daily -DailyFrequency 01:00:00 -DailyStart 06:00


Set-SCDWJobSchedule -JobName Transform.Common -ScheduleType Weekly -WeeklyFrequency Tuesday, Thursday -WeeklyStart 06:00
```

Note

To run Windows PowerShell cmdlets, the execution policy must be set to RemoteSigned. For more information, see Getting Started with the Service Manager Cmdlets in the Deployment Guide for System Center 2012 – Service Manager.

In the following procedure, you configure a schedule for the Transform job to run every 45 minutes, starting at 2:00 in the morning. However, you can modify the commands to set your own schedule.

To configure a schedule for data warehouse jobs

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. At the Windows PowerShell prompt, type the following command, and then press ENTER.

```
Set-SCDWJobSchedule -JobName Transform.Common -ScheduleType
Daily –DailyFrequency 00:45:00 –DailyStart 02:00
```

To validate a data warehouse job schedule

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. Type the following command, and then press ENTER:

```
Get-SCDWJobSchedule
```

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to Process All Dimensions in the Data Warehouse Using Windows PowerShell Cmdlets

You can process all the dimensions in the data warehouse in one operation using Windows PowerShell cmdlets, instead of processing each dimension individually. On the server that hosts SQL Server Analysis Services (SSAS), use the following Windows PowerShell script. Be sure to specify the fully qualified server name. You can type each command separately, or you can save them all as a Windows PowerShell script (.ps1) file and then run the script.

Before you can use Service Manager cmdlets, you need to configure the Service Manager Shell. For information about configuring the Service Manager Shell, see Configuring and Using the System Center 2012 - Service Manager Cmdlets for Windows PowerShell.

To process all dimensions using cmdlets

1. Copy and paste the following code snippets at the prompt in a Service Manager Shell:

   a.

   b.

   c.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to View Data Warehouse Job History

A history of data warehouse jobs is collected as they run in System Center 2012 – Service Manager. You can view this history to determine how long a job ran or to determine the last time the job ran successfully. When you display the data warehouse job history, you display the number of entries that you specify by using the *NumberOfBatches* parameter. Use the following procedure to view the last five entries in the history of a data warehouse job.

To view the last five entries in the data warehouse job history

1. On the computer that hosts the data warehouse management server, click **Start**, point to **All Programs**, click **Microsoft System Center**, click **Service Manager 2012**, and then click **Service Manager Shell**.
2. Type the following command, and then press ENTER.

```
Get-SCDWJob -NumberOfBatches 5
```

3. Type **exit**, and then press ENTER.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to Troubleshoot a Data Warehouse Job

In System Center 2012 – Service Manager, after the Data Warehouse Registration Wizard is complete and after Reporting becomes available in the Service Manager console, you can start running reports. If you encounter a problem with reports (for example, the incident management report you run does not show the current data), you can use Windows PowerShell cmdlets to troubleshoot the problem. For example, you can use the following procedure to determine whether a transform job failed, and you can evaluate any error messages that the transform job created.

To troubleshoot data warehouse jobs by using Windows PowerShell cmdlets

1. On the computer that hosts the data warehouse management server, click **Start**, click **All Programs**, click **All Programs**, click **Accessories**, and then click **Windows PowerShell**.
2. Type the following command, and then press ENTER.

```
Get-SCDWJob
```

3. Review the output, and locate any job with a status of "Failed."
4. Type the following command, and then press ENTER. In the command, specify the data warehouse job that failed as the value of the *JobName* parameter.

```
Get-SCDWJobModule -JobName Transform.Common
```

5. In the output, locate a status of "Failed," and then review the **Error Message** column for more information about why the data warehouse job failed.

6. When you are ready to retry the failed job, in the Service Manager console, click **Data Warehouse**.
7. Expand **Data Warehouse**, and then click **Data Warehouse Jobs**.
8. In the **Data Warehouse Jobs** pane, select the failed job in the list, and then click **Resume** in the **Tasks** list.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

How to Configure Microsoft SharePoint for Analytics

Microsoft SharePoint 2010 not only stores Excel workbooks that contain Service Manager Microsoft Online Analytical Processing (OLAP) data cubes in document libraries, but it is also used to render Excel workbooks with the use of a web browser. Using SharePoint makes it possible for Service Manager users that do not have Excel to get access to the information they need. It also enables quick and easy access from mobile devices.

Note

You must already have Microsoft SharePoint 2010 for Internet Sites Enterprise installed to perform this procedure.

To enable Excel Services on SharePoint 2010

1. Click **Start**, and then click **SharePoint 2010 Central Administration**.
2. Under **System Settings**, click **Manage farm features**.
3. Ensure that both the **Excel Services Application View Farm Feature** and **Excel Services Application Web Part Farm Feature** are set to **Active**. If they are not set to **Active**, click **Activate**.

See Also

Managing the Data Warehouse in System Center 2012 - Service Manager

Managing the System Center 2012 - Service Manager Self-Service Portal

The Self-Service Portal in System Center 2012 – Service Manager is used by end users to contact help desk personnel for help requests. Users can also search the knowledge base, perform tasks, and manage their requests.

Use the procedures in the following topics to manage portal pages and links.

Managing Self-Service Portal Topics

- How to Configure Concurrent Sessions and Calls

Describes how to configure concurrent sessions and calls.

- How to Modify the Self-Service Portal Attachment File Size

  Describes how to modify the Self Service Portal attachment file size.
- Customizing the Self Service Portal

  Provides an overview of customizing the Self-Service Portal.
- Enabling Tracing and Debugging for the Self Service Portal

  Explains when tracing and debugging is used to troubleshoot the Self-Service Portal.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Configure Concurrent Sessions and Calls

By limiting the number of concurrent calls and sessions on the Web Content Server in System Center 2012 – Service Manager, you can limit the number of resources used by the Self-Service Portal. Use the following procedure to configure the number of concurrent calls and sessions. For more information, see the MSDN article <serviceThrottling.

To configure concurrent calls and sessions

1. Log in to the computer hosting the Web Content Server with administrative privileges.
2. Using a text editor of your choosing (for example, Notepad), open the Web.cofig file in the %inetroot%\inetpub\wwwroot\System Center Service Manager Portal\servicehost folder.
3. Locate the <serviceBehaviors> section, as shown in the following example:

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="DefaultHttpServiceBehavior">
<serviceMetadata httpGetEnabled="true"/>
<serviceDebug includeExceptionDetailInFaults="true"/>
<dataContractSerializer maxItemsInObjectGraph="2147483647"/>
</behavior>
<behavior name="DefaultHttpsServiceBehavior">
<serviceMetadata httpsGetEnabled="true"/>
<serviceDebug includeExceptionDetailInFaults="true"/>
```

```
<dataContractSerializer maxItemsInObjectGraph="2147483647"/>
</behavior>
</serviceBehaviors>
</behaviors>
```

4. Add the line <serviceThrottling maxConcurrentCalls="160" maxConcurrentSessions="10000"/> in both the DefaultHttpServiceBehavior and DefaultHttpsServiceBehavior sections, as shown in the following example:

```
<system.serviceModel>
<behaviors>
<serviceBehaviors>
<behavior name="DefaultHttpServiceBehavior">
<serviceMetadata httpGetEnabled="true"/>
<serviceThrottling maxConcurrentCalls="160"
maxConcurrentSessions="10000"/>
<serviceDebug includeExceptionDetailInFaults="true"/>
<dataContractSerializer maxItemsInObjectGraph="2147483647"/>
</behavior>
<behavior name="DefaultHttpsServiceBehavior">
<serviceMetadata httpsGetEnabled="true"/>
<serviceDebug includeExceptionDetailInFaults="true"/>
<serviceThrottling maxConcurrentCalls="160"
maxConcurrentSessions="10000"/>
<dataContractSerializer maxItemsInObjectGraph="2147483647"/>
</behavior>
</serviceBehaviors>
</behaviors>
```

5. Close your text editor, and save the changes.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Modify the Self-Service Portal Attachment File Size

By default, users can attach files in requests that they submit when they use the Self-Service Portal in System Center 2012 – Service Manager. However, the Self-Service Portal limits the attachment file size to 10 megabytes (MB). You can modify the Self-Service Portal default attachment file size by editing a property manually in the Web.config file.

Note

The maximum file size that the Self-Service Portal supports is independent of the work item maximum size settings that are specified in the Service Manager console in the Administration workspace.

To modify the Self-Service Portal attachment file size

1. Log in to the computer that hosts the Web Content Server with administrative credentials.
2. Using a text editor of your choice (for example, Notepad), open the Web.config file in the %inetroot%\inetpub\wwwroot\System Center Service Manager Portal\servicehost folder.
3. Locate the <binaryMessageEncoding> section, as shown in the following example:

```
<binaryMessageEncoding>
        <readerQuotas maxArrayLength="10485760"/>
       </binaryMessageEncoding>
```

4. Modify the line `<readerQuotas maxArrayLength="10485760"/>` by replacing the `maxArrayLength` value with a value of your choice.
5. Close the text editor, and save the changes.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

Customizing the Self Service Portal

You can customize the Self-Service Portal in System Center 2012 – Service Manager to better suit your organization. Example customizations presented in this section are somewhat limited; they include changes to formatting and adding a SharePoint list. However, the Self-Service Portal is based on SharePoint web services, so you can make additional customizations on your own, outside the scope of this section.

Use the procedures in the following topics to customize the Self-Service Portal.

Self-Service Portal Customization Topics

- How to Update the Portal Title and Image

  Describes how to update the Self-Service Portal's tile and associated logo.
- How to Add Navigation Links

  Describes how to add navigational links to the Self-Service Portal.
- How to Update the Portal Theme

  Describes how to update the theme for the entire Self-Service Portal.
- How to Add a Portal Announcement Page

  Describes how to add an announcement page using a SharePoint list.
- How to Modify the Help Article Web Part

Describes how to modify a specific web part in the Self-Service Portal.

- How to Modify a Master Page File

  Describes how to modify a master page file using SharePoint Designer.

- How to Select the Self Service Portal Language

  Describes how to select the localized languages that are displayed in the Self-Service Portal based on a user's choice.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Update the Portal Title and Image

You can make limited customizations to the SharePoint Web parts that make up the Self-Service Portal. You can customize the left pane navigational elements, the home page title, image, and the web-parts that present data to the web user by using the **Site Actions** menu on **Site Pages**. By using this procedure, you can make changes to the following items to customize the Self-Service Portal for your environment:

- Title
- Image

To update the portal title and image

1. Start a browser and connect to the Self-Service Portal home page, for example, *http://<SiteName>:81/SMPortal*.
2. In the upper left corner, click **Site Actions**, and then click **Site Settings**.
3. On the **Site Settings** page, in the **Look and Feel** area, click **Title, description, and icon**.
4. Follow the on-screen directions to change the title, logo, and website address, and then click **OK**.

   Note

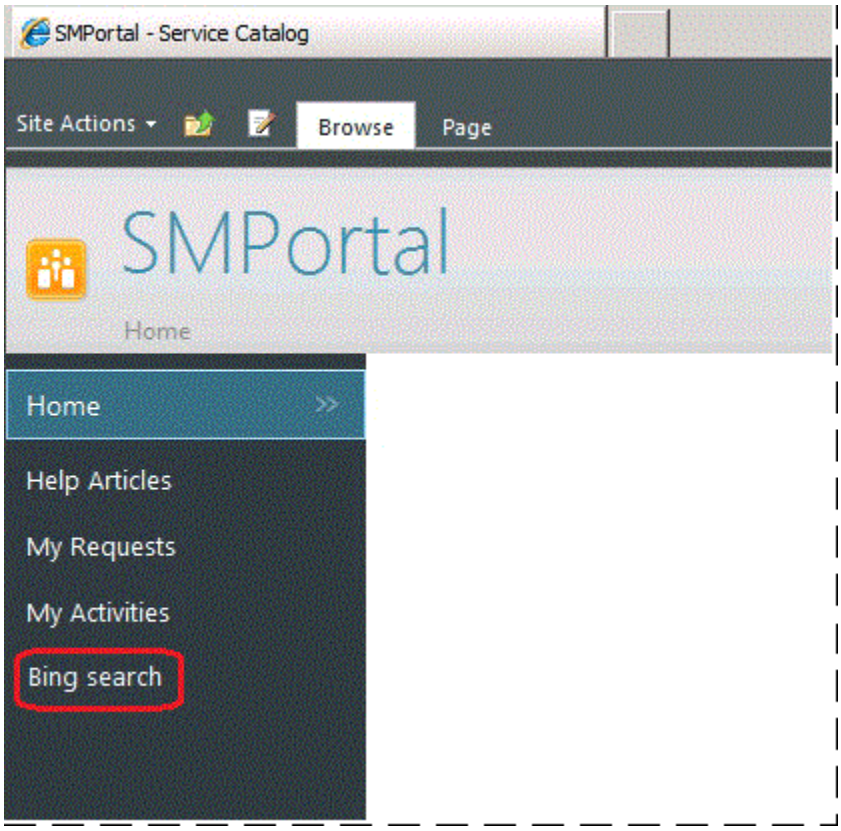
   In this guide, it is assumed that the website name is SMPortal, and all of the examples in this guide use SMPortal in all path statements. If you change the website name, you must adjust the examples that are presented in this guide.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Add Navigation Links

You can add additional navigation links to the Self-Service Portal home page in System Center 2012 – Service Manager. As an example, the following procedure adds a link titled "Bing search" to an external website (http://www.bing.com), as shown in the following illustration.



To add navigation links

1. Start a browser, and connect to the Self-Service Portal home page, for example, http://<WebServerName>:82/SMPortal.
2. In the upper left corner, click **Site Actions**, and then click **Site Settings**.
3. On the **Site Settings** page, in the **Look and Feel** area, click **Quick launch**.
4. On the **Quick Launch** page, click **New Navigation Link**.
5. In the **Type the Web address** field, type **http://www.bing.com**.
6. In the **Type the description** field, type **Bing search**, and then click **OK**.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Update the Portal Theme

You can update the color theme used by the Self-Service Portal in System Center 2012 – Service Manager. As an example, the following procedure changes the color theme from the default theme to one of your choice.

To update the portal theme

1. Start a browser, and connect to the Self-Service Portal home page, for example, http://<WebServerName>:82/SMPortal.
2. In the upper left corner, click **Site Actions**, and then click **Site Settings**.
3. On the **Site Settings** page, in the **Look and Feel** area, click **Site theme**.
4. On the **Site Theme** page, select the theme of your choice in the theme list, and then click **Apply**. For example, select **Azure**.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Add a Portal Announcement Page

You can add a new page on the Self-Service Portal in System Center 2012 – Service Manager for administrative announcements. As an example, the following procedures add an announcement page, and then you add an announcement, informing end users that the Help Desk will be closed on New Year's Day.

To add an announcement page

1. Start a browser, and connect to the Self-Service Portal home page, for example, http://<WebServerName>:82/SMPortal.
2. In the upper left corner, click **Site Actions**, and then click **Site Settings**.
3. On the **Site Settings** page, in the **Look and Feel** area, click **Quick launch**.
4. On the **Quick Launch** page, click **New Navigation Link**.
5. In the **Type the Web address** field, type **/SMPortal/Lists/Announcements/AllItems.aspx**, and then in the description box, type **Announcements**.
6. Click **OK**, and then navigate to the home page.

To create an announcement

1. Start a browser, and connect to the Self-Service Portal home page, for example, http://<WebServerName>:82/SMPortal.
2. Click **Announcements**.
3. On the **Announcements – All items** page, click **Add new announcement**.
4. In the **Title** box, type a name for the announcement. For example, type **Help Desk Closed New Year's Day**.

5. In **Body**, you can type additional information for the announcement.
6. Optionally, you can set an expiration date by selecting the date in the **Expires** box. For example, you can set the **Expires** date to January 2nd.
7. Click **Save** to close the announcement.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Modify the Help Article Web Part

You can edit SharePoint Web parts of the Self-Service Portal in order to modify the Service Manager help article web part, which end users use to search for knowledge articles. However, customization is limited in this example.

To modify the help article web part

1. Start a browser, and connect to the Self-Service Portal home page, for example, http://<WebServerName>:82/SMPortal.
2. Click **Help Articles**, and then in the upper left corner, click **Site Actions**.
3. Click **Edit Page**, and on the right side of page, click the down-pointing arrow, and then click **Edit Web Part**.
4. In the **KnowlegeArticleWebPart** box, do the following:
   a. In the **Page** area, type a value for **Background Color**. For example, type **FF0890E5**.
   b. In the **Page Title** area, type a value for **Foreground Color**. For example, type **FFAA0000**.
   c. Type a value for **Font Family**. For example, type **Courier New**.
   d. Type a value for **Font Size**. For example, type **24**.
   e. Select a value for **Font Style**. For example, select **Bold**.
   f. Optionally, modify any other properties as desired.
5. Click **OK** to close the **Edit Web Part** box, and then click **Save & Close** to close the Web part page editor.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Modify a Master Page File

You can edit some web elements of the Self-Service Portal using Microsoft SharePoint Designer 2010. You can use SharePoint Designer 2010 to modify SharePoint master pages and style sheets. However, customization is limited in this example to formatting. In any of the following example modifications, you can choose customizations that better fit your organization.

Note

You should have SharePoint Designer 2010 installed before you use the following procedure. However, you can download SharePoint Designer 2010 from the Microsoft Download Center if you do not already have it installed.

To modify a master page file

1. Start a browser, and connect to the Self-Service Portal home page, for example, http://<WebServerName>:82/SMPortal.
2. In the upper left corner, click **Site Actions**, and then select **Edit in SharePoint Designer**.
3. In the navigation pane, select **Master Pages**, and then in the **Master Pages** list, select **SMPortalPage.master**.
4. In the **Customization** area, click **Edit file** to open it in the **Advanced Editor**.
5. Select the title in the design window, and then in the **Tag Properties** pane, under **Appearance**, expand **Font**.
6. Click the box to the right of **Name**, and then select **Times New Roman**.
7. In the lower-left portion of SharePoint Designer 2010, click **Split** to show both the preview pane and the XHTML view of the master file.
8. Click the **Layout** menu tab, and then click **Manage Layers**.
9. In the **Layers** list, select **s4-workspace**. The XHTML view appears and selects the corresponding code.
10. At the top of the selected code, right click the code ** **, and then click **Follow Code Hyperlink** to open the CSS file that is associated with the master file.
11. In the CSS file, look for the section labeled `Body{` near the top of the XHTML code, and then under `height:100%`, insert a new line and type **background-color:#006600**.
12. Save the CSS and SMPortalPage.master files that you have updated, and then close SharePoint Designer 2010.
13. Refresh your view of the Self-Service Portal to view the changes that you have made.

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

How to Select the Self Service Portal Language

Service Manager does not include a localized Self Service Portal SharePoint template. As a result, after you install the Self-Service Portal on a non-English SharePoint site, it will contain content that is not localized. In order to display the Self-Service Portal in a fully localized language, you must modify the Self Service Portal to suit your organization's needs.

In System Center 2012, because the portal is based on SharePoint 2010, it is possible for your end-users to choose the languages they want displayed by themselves, subject to the SharePoint administrator's configuration.

You can also set up multiple SharePoint sites for the Self-Service Portal which can have different default languages and then you can direct users to a particular portal if you want. End-users can

still change their language to whatever language they want, as long as the administrator has enabled it on the site.

To select the Self-Service Portal language

1. Install whatever language packs you want for your SharePoint product site and then follow instructions to install and deploy them using of the following options.
   - Download SharePoint 2010 Server Language packs and then read and follow the installation and deployment instructions.
   - Download SharePoint 2010 Foundation language packs and then read and follow the installation and deployment instructions.
2. Once you have the language packs deployed you can configure the language settings. As a SharePoint site administrator, open the Self-Service Portal home page, click **Site Actions** and then select **Site Settings**.
3. Under **Site Administration**, click **Language settings** and select your default language and additional languages you want to enable and then click **OK**.
4. Click **Site Actions**, select **Site Settings** and then click **Quick Launch** and then modify items such as **Home**, **Help Articles**, **My Requests**, and **My Activities** for your language.
5. Click **Site Actions**, select **Site Settings** and then click **Site Libraries and lists** and open each item, such as **Customize Calendar** and then modify items such as title, description and navigation and associated columns headings.
6. Separately, each individual user can choose the language they want to display in the Self-Service Portal, under <Account Name> by selecting **Select Display Language** and then click the language they want to display.

Enabling Tracing and Debugging for the Self Service Portal

By default, Service Manager disables debugging and tracing for the Self-Service Portal (ASP.NET pages) and for the Service Manager Web service (an ASP.NET application). When contacting Microsoft Product Support Services, they might ask you to enable tracing and debugging for troubleshooting purposes. For more information about debugging and enabling tracing for ASP.NET pages and applications see the following topics:

- ASP.NET Debugging Overview
- ASP.NET Tracing Overview
- How to: Enable Tracing for an ASP.NET Page
- How to: Enable Tracing for an ASP.NET Application
- How to: Enable Debugging for ASP.NET Applications

See Also

Managing the System Center 2012 - Service Manager Self-Service Portal

Using Service Manager Tasks to Troubleshoot Computer Problems

If you want to view the logs on a remote computer that is exhibiting problems, you must first create a task that opens Event Viewer. Event Viewer reads logs from remote computers.

In System Center 2012 – Service Manager, administrators can create and use tasks to automate and simplify lengthy, complex, or repetitive processes. Operators typically use tasks to help troubleshoot user incidents. After creating a task, operators can run the task directly from the Service Manager console.

Important

In this release, to create a task, the logged-on user must have administrative credentials.

The Event Viewer task that you create will display logs from the computer that is identified as a configuration item in the incident. The help desk analyst can then select an incident in the Service Manager console and run this task for the computers that are related to the incident.

Using Tasks to Troubleshoot Problems Topics

- How to Create a Task

  Describes how to create a task.
- How to Run a Task from an Incident View

  Describes how to run a task from an incident view.

Other Resources for This Component

- TechNet Library main page for System Center 2012 – Service Manager
- Administrator's Guide for System Center 2012 – Service Manager
- Planning Guide for System Center 2012 – Service Manager
- Operations Guide for System Center 2012 – Service Manager

How to Create a Task

Use the following procedures in System Center 2012 – Service Manager to create a task—for example, a task that you can use to open Event Viewer and view logs on a computer—and then validate the new task. Event Viewer displays the logs from the remote computer that is listed as a Configuration Item in the incident.

To create a task

1. In the Service Manager console, click **Library**.
2. On the **Library** pane, expand **Library**, and then select **Tasks.**
3. On the **Tasks** pane, select **Create Task**.
4. On the **Before You Begin** page, click **Next**.

5. On the **General** page, do the following:
   a. In the **Task name** box, type a name for the task. For example, type **Event Viewer**.

      Note
      In this release, if you edit and change any of the properties of a task, you have to close and reopen the console before you can view the task.

   b. Next to the **Target class** area, click the ellipsis button (**…**).
   c. In the **Choose Class** dialog box, in the **Class** list, click **Incident**, and then click **OK**.
   d. In the **Management pack** list, make sure that **Service Manager Incident Management Configuration Library** is selected, and then click **Next**.

      Note
      In this release, if you select the option to create a new management pack, you have to close and reopen the console before you can view this task.

6. On the **Display Task by Category** page, select the category where the task will be displayed. For example, select **Incident Management Folder Tasks**, and then click **Next**.
7. On the **Command Line** page, do the following:
   a. In the **Full path to command** box, type the full path of the command you want to run with this task. For example, type **%windir%\system32\eventvwr.exe**.
   b. In the **Parameters** area, click **Insert Property**.
   c. In the **Select Property** dialog box, in the **Related classes** list, expand **Incident**, and then click **Is Related to Configuration Item**.
   d. In the **Available Properties** box, type **Computer Name**.
   e. Under **Windows Computer**, click **NetBIOS Computer Name**, and then click **Add**.
   f. Optionally, select **Log in action log when this task is run** to add information to the incident action log when the task runs, and then click **Next**.
8. On the **Summary** page, click **Create**.
9. On the **Completion** page, observe that **The new task was created successfully** appears, and then click **Close**.

To validate a new task

1. In the Service Manager console, click **Work Items**.
2. In the **Work Items** pane, expand **Work Items**, expand **Incident Management**, and then click **All Incidents**.
3. In the **All Incidents** pane, click an incident for which a computer name has been entered as a configuration item.
4. In the **Tasks** pane, under the name of the incident you selected in the previous step, click **Event Viewer**.
5. Notice that Event Viewer starts, and the events from the computer that are associated with the incident are displayed.

You can use the Get-SCSMTask Windows PowerShell command to view Service Manager tasks.

See Also

Using Service Manager Tasks to Troubleshoot Computer Problems

How to Run a Task from an Incident View

Use the following procedure to run a task, such as the Ping task, from an Incident view in System Center 2012 – Service Manager.

To run a task from an Incident view

1. In the Service Manager console, click **Work Items**, and then select any Incident Management view. Select an incident in the view, and notice that in the **Tasks** pane, under **<Incident Name>**, the **Ping Related Computer** task appears.
2. In the **Tasks** pane, click the task to run it. For example, **Ping Related Computer**. If a computer is not associated with the incident, you must specify the name of the computer to run the task on. If more than one computer is associated with an incident, choose one computer to run the task on.
3. If the task logs actions into the action log, you can open the incident and view the action log to see the output that the task generated.
4. If the **Console Task Output - <Task Name>** box appears, verify the output generated by the task, and then click **Close**.

See Also

Using Service Manager Tasks to Troubleshoot Computer Problems

To Configure System Center 2012 - Service Manager CEIP Settings

During setup in System Center 2012 – Service Manager, on the **Help improve System Center** page, you have the option to participate in the Customer Experience Improvement Program (CEIP). For a Service Manager management server, you can use the first following procedure to let Service Manager participate in the program or remove Service Manager from this program. For either a data warehouse management server or Service Manager management server, you use the second following procedure to modify the registry to join or leave the Customer Experience Improvement Program.

To configure Service Manager CEIP settings using the Service Manager console

1. In the Service Manager console, in the toolbar, click **Help**.
2. In the **Help** menu, you can choose to either let Service Manager join the program or

remove Service Manager from the program: Observe the entry **Join the Customer Experience Improvement Program**, and then do one of the following:

- If a check mark is displayed, click **Join the Customer Experience Improvement Program** to remove Service Manager from the CEIP program.
- If the check mark is not displayed, click **Join the Customer Experience Improvement Program** to join the CEIP program, and then in the System Center Service Manager dialog box, click **Yes** to confirm your decision.

To configure CEIP settings using the registry

1. On the Service Manager management server or data warehouse server, open Registry Editor.
2. Create the following registry key if it does not already exist.

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\SCSM
3. Create the following DWORD (32-bit) Value if it does not already exist.

   CEIPEnable
4. Set the value to 1 to participate in the CEIP or set the value to 0 to leave the CEIP.

See Also

Administering System Center 2012 - Service Manager

Appendix A - List of User Role Profiles in System Center 2012 - Service Manager

This appendix provides detailed information about the scope and properties of user role profiles in System Center 2012 – Service Manager.

EndUser

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	Object Templates
Create	• Work Item • Work Item Log • File Attachm	All for the specified types.	All for the specified types.	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
	ent • Reviewer • User Preference			
Update	• File Attachment • Work Item Log • Star Rating	All for the specified types.	• DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • WorkItemRelatesToWorkItem->WorkItem • WorkItemRelatesToRequestOffering->RequestOffering • WorkItemRelatesToConfigItem->ConfigurationItem • WorkItemAboutConfigItem->ConfigurationItem	None
Delete	None	None	None	None

ReadOnlyOperator

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• User Preference • Personal Notification	All for the specified types.	All for the specified types.	None
Update			• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • WorkItemRelatesToRequestOffering->RequestOffering • WorkItemRelatesToWorkItem->WorkItem	None
Delete	None	None	None	None

IncidentResolver

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Incident • Manual Activity • File Attachment • Work Item Log • User Preference • Personal Notification	All for the specified types.	All for the specified types.	None
Update	• File Attachment • Work Item Log • Manual Activity • Star Rating	All for the specified types.	• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • WorkItem.BillableTimeHasWorkingUser->User	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
			• WorkItem.IncidentPrimaryOwner->User • WorkItem.TroubleTicketResolvedBy User->User • WorkItem.TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User	
Delete	• File Attachment • Manual Activity	All for the specified types.	All for the specified types.	None

ChangeInitiator

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Change Request • Activity • File Attachment • Work Item Log • Reviewer • User Preference • Personal Notification	All for the specified types.	All for the specified types.	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Update	Star Rating	All for the specified types.	• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • WorkItemAboutCatalogItem->CatalogItem	None
Delete	None	None	None	None

ActivityImplementer

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Create	• User Preference • Personal Notification	All for the specified types.	All for the specified types.	None
Update	Star Rating	• ManualActivity.Status • ManualActivity.Notes	• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Delete	None	None	None	None

ProblemAnalyst

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Problem • File Attachment • Work Item Log • User Preference • Personal Notification	All for the specified types.	All for the specified types.	None
Update	• Problem • File Attachment • Work Item Log • Star Rating	All for the specified types.	• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser-	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
			>User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User	
Delete	File Attachment	All for the specified types.	All for the specified types.	None

ServiceRequestAnalyst

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	All for the specified types.	All for the specified types.	All for the specified types.	None
Update	• Service Request • Activity • File Attachment • Work Item Log • Reviewer		• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • Knowledge.DocumentHasAverageRating->KnowledgeArticle • WorkItemAffectedUser->User • UserHasPreference->User	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
	• Star Rating		• WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • WorkItemRelatesToRequestOffering->RequestOffering	
Delete	• Activity • File Attachment • Reviewer	All for the specified types.	All for the specified types.	None

ReleaseManager

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Release Record • Activity • File Attachment • Work Item Log • Reviewer • User Preference • Personal Notification	All for the specified types.	All for the specified types.	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Update	• Release Record • Activity • File Attachment • Work Item Log • Reviewer • Star Rating	All for the specified types.	• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • DocumentHasAverageRating->KnowledgeArticle • WorkItemAffectedUser->User • UserHasPreference->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User	None
Delete	• Activity • File Attachment • Reviewer	All for the specified types.	All for the specified types.	None

ChangeManager

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Change Request • Activity	All for the specified types.	All for the specified types.	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
	• File Attachment • Work Item Log • Reviewer • User Preference • Personal Notification			
Update	• Change Request • Change Request • Activity • File Attachment • Work Item Log • Reviewer • Star Rating	All for the specified types.	• WorkItemAboutConfigItem->ConfigurationItem • WorkItemRelatesToConfigItem->ConfigurationItem • EntityLinksToKnowledgeDocument->ConfigurationItem • WorkItemRelatesToWorkItem->WorkItem • Knowledge.DocumentHasAverageRating->KnowledgeArticle • WorkItemAffectedUser->User • UserHasPreference->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • WorkItem.BillableTimeHasWorkingUser->User • WorkItem.IncidentPrimaryOwner->User •	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
			WorkItem.TroubleTicketResolvedBy User->User • WorkItem.TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • WorkItemAboutCatalogItem ->CatalogItem	
Delete	• Activity • File Attachment • Reviewer	All for the specified types.	All for the specified types.	None

AdvancedOperator

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Work Item • Configuration Item • Announcement • File Attachment • Work Item Log • Reviewer • User Preference	All for the specified types.	All for the specified types.	None

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
	• Personal Notification			
Update	• Work Item • Configuration Item • Announcement • File Attachment • Work Item Log • Reviewer • User Preference	All for the specified types.	• Knowledge.DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • WorkItemRelatesToRequestOffering->RequestOffering	None
Delete	• Announcement • Activity • Reviewer • File Attachment	All for the specified types.	All for the specified types.	None

Author

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Work Item • Configu	All for the specified	All for the specified types.	• Template • View

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
	ration Item • Catalog Item • Announcement • File Attachment • Work Item Log • Reviewer • User Preference • Personal Notification	types.		• Folder • Enumeration
Update	• Work Item • Configuration Item • Catalog Item • Announcement • File Attachment • Work Item Log • Reviewer • Star Rating		• DocumentHasAverageRating->KnowledgeArticle • UserHasPreference->User • WorkItemAffectedUser->User • WorkItemAssignedToUser->User • WorkItemCreatedByUser->User • FileAttachmentAddedByUser->User • BillableTimeHasWorkingUser->User • IncidentPrimaryOwner->User • TroubleTicketResolvedByUser->User • TroubleTicketClosedByUser->User • ReviewerIsUser->User • ReviewerVotedByUser->User • ServiceOfferingRelatesToRequestOffering->RequestOffering	• Template • View • Folder • Enumeration
Delete	• Activity • Reviewer • File Attachment • Announ	All for the specified types.	All for the specified types.	• Template • View • Folder • Enum

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
	cement			eration

Workflow

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	All	All	All	All
Create	• Work Item • Configuration Item • Announcement • File Attachment • Work Item Log • Reviewer • SLA Information • Admin Item SLA • User Preference	All for the specified types.	All for the specified types.	None
Update	• Work Item • Configuration Item • Announcement • File Attachment • Work Item Log • Reviewer • SLA Information • Admin Item SLA • Star Rating	• System.Knowledge.DocumentHasAverageRating • System.UserHasPreference • System.WorkItemAffectedUser • System.WorkItemAssignedToUser • System.WorkItemCreatedByUser • System.FileAttachmentAddedBy User • System.WorkItem.BillableTimeHasWorkingUser	None	

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
		• System.WorkItem.IncidentPrimaryOwner • System.WorkItem.TroubleTicketResolvedByUser • System.WorkItem.TroubleTicketClosedByUser • System.ReviewerIsUser • System.ReviewerVotedByUser		
Delete	DCM_NonCompliance_CI	All for the specified types.	All for the specified types.	None

ReportUser

Operation	Instance Type Scope	Properties	Relationships	Presentational Elements Scope
Read	SRS Resource Store	All for the specified type	All for the specified type	None
Create	Personal Notification	All for the specified type	All for the specified type	None
Update	None	None	None	None
Delete	None	None	None	None

ImpliedIncidentAffectedUser

The permissions for the implied Affected User profile are granted through the WorkItemAffectedUser relationship.

Operation	Type	Property	Relationship
Read	Incident or service	All properties of an	All relationships that include the

Operation	Type	Property	Relationship
	request instances, and anything that is contained within.	incident instance.	incident or service request instance.
Create	Work items that the user is affected by: • Work item log • File attachment	All properties of a work item log and a file attachment for the incident or service request instance.	File attachment for an incident or service request instance.
Update	Work items that the user is affected by: • Incident • Service request • Work item log • File attachment	All properties of an incident or service request instance.	Incident instance BillableTimeHasWorkingUser->User.
Delete	Work item that the user is affected by - File attachment	File attachment for an incident or service request instance.	File attachment for an incident or service request instance.

ImpliedReviewer

The permissions for the implied Review Activity Reviewer profile are granted through the ReviewerIsUser relationship.

Operation	Type	Property	Relationship
Read	Reviewer instances and anything that is contained within.	All properties of a Reviewer instances and anything that is contained within.	All relationships that include the Reviewer instance, and anything that is contained within.
Create	None	None	None
Update	None	Reviewer instances: • Reviewer.Comments • Reviewer.DecisionDate • Reviewer.Decision	Reviewer Instances: • ReviewerVotedByUser->User • ReviewerVotedByUser-

Operation	Type	Property	Relationship
			>Reviewer
Delete	None	None	None

ImpliedActivityEditor

The permissions for the implied Assigned To User profile are granted through the WorkItemAssignedToUser relationship.

Operation	Type	Property	Relationship
Read	Activity instances and anything that is contained in it.	None	None
Create	Work item instances that the user is assigned to: • Activity • Reviewer	All properties of Activity and Reviewer instances that are related to a work item instance.	All the Activity and Reviewer instances that are related to a work item Instance.
Update	Work item instances that the user is assigned to: Activity	All properties of an activity and the work item instances.	All Activity instances that are related to the work item Instance.
Delete	None	None	None

ImpliedConfigItemCustodian

The permissions for the implied **CI Owner** profile are granted through the **ConfigItemOwnedByUser** relationship.

Operation	Type	Property	Relationship
Read	Configuration item instances and anything that is contained within.	All properties of a configuration item instance and anything that is contained in it.	All relationships that include a configuration item instance, and anything that is contained in it.
Create	None	None	None
Update	None	None	Configuration item Instance - WorkItemAboutConfigItem

Operation	Type	Property	Relationship
Delete	None	None	None

ImpliedPrimaryComputerUser

The permissions for the implied CI Primary User profile are granted through the ComputerPrimaryUser relationship.

Operation	Type	Property	Relationship
Read	Configuration item instances and anything that is contained within.	All properties of a configuration item instance and anything that is contained within.	All relationships that include the configuration item instance and anything that is contained within.
Create	None	None	None
Update	None	None	None
Delete	None	None	None

Appendix B - Mapping Active Directory Domain Services Attributes to Properties in System Center 2012 - Service Manager

Using an Active Directory connector, System Center 2012 – Service Manager synchronizes data with the User, Group, Computer, and Printer Active Directory Domain Services (AD DS) objects. The following tables describe the mapping between the attributes of the Active Directory objects and the corresponding Service Manager class properties.

User/Microsoft.AD.User

The following table describes the mapping between the attributes of the Active Directory User object and the Service Manager **Microsoft.AD.User** class properties.

Active Directory user attribute	Microsoft.AD.User property
physicaldeliveryofficename	Office
displayname	displayname

Active Directory user attribute	Microsoft.AD.User property
company	Company
employeeid	Employeeid
department	Department
telephonenumber	BusinessPhone
homePhone	HomePhone
facsimileTelephoneNumber	Fax
mobile	Mobile
pager	Pager
mail	Email
givenname	FirstName
initials	Initials
sn	LastName
distinguishedname	Distinguishedname
title	Title
manager	manager
samaccountname	UserName
l	City
StreetAddress	StreetAddress
st	State
postalCode	Zip
co	Country
localeID	Locale
msRTCSIP-PrimaryUserAddress	SipAddress
objectSid	SID
Domain	Domain

Group/Microsoft.AD.UserBase

The following table describes the mapping between the attributes of the Active Directory Group object and the Service Manager **Microsoft.AD.UserBase** class properties.

Active Directory group attribute	Microsoft.AD.UserBase property
displayname	displayname
mail	Email
distinguishedname	Distinguishedname
samaccountname	samaccountname
objectSid	SID
Domain	Domain

Printer/Microsoft.AD.Printer

The following table describes the mapping between the attributes of the Active Directory PrintQueue object and the Service Manager **Microsoft.AD.Printer** class properties.

Active Directory printer attribute	Microsoft.AD.Printer property
uNCName	uNCName
serverName	serverName
shortServerName	shortServerName
printerName	printerName
printNetworkAddress	printNetworkAddress
printShareName	printShareName
isDeleted	isDeleted
driverName	driverName
driverVersion	driverVersion
printMemory	printMemory
printCollate	printCollate
printOwner	printOwner
assetNumber	assetNumber
managedBy	managedBy

Active Directory printer attribute	Microsoft.AD.Printer property
printDuplexSupported	printDuplexSupported
printColor	printColor
printStaplingSupported	printStaplingSupported
versionNumber	versionNumber
url	url
printMediaSupported	printMediaSupported
printRateUnit	printRateUnit
printMaxXExtent	printMaxXExtent
printKeepPrintedJobs	printKeepPrintedJobs
printRate	printRate
printMediaReady	printMediaReady
printPagesPerMinute	printPagesPerMinute
printMaxResolutionSupported	printMaxResolutionSupported
printMACAddress	printBinNames
printMACAddress	printMACAddress
portName	portName
physicalLocationObject	physicalLocationObject
keywords	keywords
printNotify	printNotify
wWWHomePage	wWWHomePage
whenChanged	whenChanged
modifyTimeStamp	modifyTimeStamp
location	location
canonicalName	canonicalName
displayname	displayname
cn	Fullname
distinguishedname	Distinguishedname
description	description

Computer/Microsoft.Windows.Computer

The following table describes the mapping between the attributes of the Active Directory Computer object and the Service Manager **Microsoft.Windows.Computer** class properties.

Active Directory computer attribute	Microsoft.Windows.Computer property
msDS-SiteName	ActiveDirectorySite
dNSHostName	DNSName
ipHostNumber	IPAddress
networkAddress	NetworkName
msDS-PrincipalName	PrincipalName
displayname	displayname
samaccountname	NetbiosComputerName
objectSid	ActiveDirectoryObjectSid
ou	OrganizationalUnit
Domain	NetbiosDomainName

Appendix C - Mapping System Center 2012 - Service Manager Properties to Configuration Manager Database Views

The hardware inventory feature in Configuration Manager gathers information about computers in the organization. In Service Manager, by using a Configuration Manager Connector, you can import that hardware inventory data from Configuration Manager. The tables in this appendix describe the mapping between Service Manager properties and column names of Configuration Manager 2007 database views.

Microsoft.SystemCenter.ConfigurationManager.DeployedComputer

The following table describes the mapping for the **Microsoft.SystemCenter.ConfigurationManager.DeployedComputer** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_COMPUTER_SYSTEM.Name0
Microsoft.SystemCenter.ConfigurationManager.DeployedComputer	HardwareID [Key]	SCCM.Ext.vex_R_System.Hardware_ID0
	SMBIOS_UUID	SCCM.Ext.vex_R_System.SMBIOS_GUID0
	SMBIOSAssetTag	SCCM.Ext.vex_GS_SYSTEM_ENCLOSURE.SMBIOSAssetTag0
	Manufacturer	SCCM.Ext.vex_GS_SYSTEM_ENCLOSURE.Manufacturer0
	Model	SCCM.Ext.vex_GS_COMPUTER_SYSTEM.Model0
	NumberOfProcessors	SCCM.Ext.vex_GS_COMPUTER_SYSTEM.NumberOfProcessors0
	SystemType	SCCM.Ext.vex_GS_COMPUTER_SYSTEM.SystemType0
	ChassisType	SCCM.Ext.vex_GS_SYSTEM_ENCLOSURE.ChassisTypes0
	SerialNumber	If SCCM.Ext.vex_GS_SYSTEM_ENCLOSURE.SerialNumber0 is NULL, '00000000' or 'Not Available', then SCCM.Ext.vex_GS_PC_BIOS.SerialNumber0, else SCCM.Ext.vex_GS_SYSTEM_ENCLOSURE.SerialNumber0

Microsoft.Windows.Computer

The following table describes the mappings for the **Microsoft.Windows.Computer** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_COMPUTER_SYSTEM.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
		Name0
Microsoft.Windows.Computer	PrincipalName (FQDN) [Key]	Constructed using SCCM.Ext.vex_GS_COMPUTER_SYSTEM.Name0 or SCCM.Ext.vex_R_System.Netbios_Name0 and SCCM.Ext.vex_GS_COMPUTER_SYSTEM.Domain0 or SCCM.Ext.vex_R_System.Resource_Domain_OR_Workgr0. If SCCM.Ext.vex_GS_COMPUTER_SYSTEM.Name0 is null, SCCM.Ext.vex_R_System.Netbios_Name0 is used as name. If SCCM.Ext.vex_GS_COMPUTER_SYSTEM.Domain0 is null, SCCM.Ext.vex_R_System.Resource_Domain_OR_Workgr0 is used as domain.
	NetbiosComputerName	SCCM.Ext.vex_R_System.Netbios_Name0
	NetbiosDomainName	SCCM.Ext.vex_R_System.Resource_Domain_OR_Workgr0
	OffsetInMinuteFromGreenwichTime	SCCM.Ext.vex_GS_Computer_System.CurrentTimeZone0
	IsVirtualMachine	SCCM.Ext.vex_GS_Computer_System.Model0, vex_GS_Manufacturer, that is, Model0 = "Virtual Machine" or "VMware Virtual Platform" OR Manufacturer="Microsoft Corporation" or "VMware, Inc"
	ActiveDirectorySite	SCCM.Ext.vex_R_System.AD_Site_Name0
	LastInventoryDate	SCCM.Ext.Vex_GS_Workstation_Status.LastHWScan

Microsoft.Windows.OperatingSystem

The following table describes the mappings for the **Microsoft.Windows.OperatingSystem** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_OPERATING_SYSTEM.Caption0
Microsoft.Windows.OperatingSystem	OSVersion	SCCM.Ext.vex_GS_OPERATING_SYSTEM.Version0
	BuildNumber	SCCM.Ext.vex_GS_OPERATING_SYSTEM.BuildNumber0
	CSDVersion	SCCM.Ext.vex_GS_OPERATING_SYSTEM.CSDVersion0
	InstallDate	SCCM.Ext.vex_GS_OPERATING_SYSTEM.InstallDate0
	SystemDrive	SCCM.Ext.vex_GS_OPERATING_SYSTEM.SystemDirectory0
	WindowsDirectory	SCCM.Ext.vex_GS_OPERATING_SYSTEM.WindowsDirectory0
	PhysicalMemory	SCCM.Ext.vex_GS_OPERATING_SYSTEM.TotalVisibleMemorySize0
	LogicalProcessors	SCCM.Ext.vex_GS_COMPUTER_SYSTEM.NmberOfProcessors0
	CountryCode	SCCM.Ext.vex_GS_OPERATING_SYSTEM.CountryCode0
	Locale	SCCM.Ext.vex_GS_OPERATING_SYSTEM.Locale0
	Manufacturer	SCCM.Ext.vex_GS_OPERATING_SYSTEM.Manufacturer0
	OSLanguage	SCCM.Ext.vex_GS_OPERATING_SYSTEM.OSLanguage0
	MinorVersion	SCCM.Ext.vex_GS_OPERATING_SYSTEM.Version0
	MajorVersion	SCCM.Ext.vex_GS_OPERATING_SYSTEM.Version0

Microsoft.Windows.Peripherals.LogicalDisk

The following table describes the mappings for the **Microsoft.Windows.Peripherals.LogicalDisk** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_LOGICAL_DISK.Name0
Microsoft.Windows.LogicalDevice	DeviceID [Key]	SCCM.Ext.vex_GS_LOGICAL_DISK.DeviceID0
	Name	SCCM.Ext.vex_GS_LOGICAL_DISK.Name0
	Description	SCCM.Ext.vex.GS_LOGICAL_DISK.Description0
Microsoft.Windows.LogicalDisk	VolumeName	SCCM.Ext.vex_GS_LOGICAL_DISK.VolumeName0
Microsoft.Windows.Peripherals.LogicalDisk	FileSystem	SCCM.Ext.vex_GS_LOGICAL_DISK.FileSystem0
	Compressed	SCCM.Ext.vex_GS_LOGICAL_DISK.Compressed0
	Size	SCCM.Ext.vex_GS_LOGICAL_DISK.Size0
	DriveType	SCCM.Ext.vex_GS_LOGICAL_DISK.DriveType0
	FreeSpace	SCCM.Ext.vex_GS_LOGICAL_DISK.FreeSpace0

Microsoft.Windows.Peripherals.PhysicalDisk

The following table describes the mappings for the **Microsoft.Windows.Peripherals.PhysicalDisk** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_DISK.Name0
Microsoft.Windows.LogicalDevice	DeviceID [Key]	SCCM.Ext.vex_GS_DISK.DeviceID0

Service Manager type	Service Manager property	Column name of Configuration Manager database views
	Name	SCCM.Ext.vex_GS_DISK.Name0
	Description	SCCM.Ext.vex.GS_DISK.Description0
Microsoft.Windows.PhysicalDisk	MediaType	SCCM.Ext.vex.GS_DISK.MediaType0
	PNPDeviceID	SCCM.Ext.vex.GS_DISK.PNPDeviceID0
Microsoft.Windows.Peripherals.PhysicalDisk	Caption	SCCM.Ext.vex.GS_DISK.Description0
	Index	SCCM.Ext.vex.GS_DISK.Index0
	InterfaceType	SCCM.Ext.vex.GS_DISK.InterfaceType0
	Manufacturer	SCCM.Ext.vex.GS_DISK.Manufacturer0
	Model	SCCM.Ext.vex.GS_DISK.Model0
	SCSIBus	SCCM.Ext.vex.GS_DISK.SCSIBus0
	SCSILogicalUnit	SCCM.Ext.vex.GS_DISK.SCSILogicalUnit0
	SCSIPort	SCCM.Ext.vex.GS_DISK.SCSIPort0
	SCSITargetID	SCCM.Ext.vex.GS_DISK.TargetId0
	Size	SCCM.Ext.vex.GS_DISK.Size0
	TotalCylinders	SCCM.Ext.vex.GS_DISK.TotalCylinders0
	TotalHeads	SCCM.Ext.Vex.GS_DISK.TotalHeads0
	TotalSectors	SCCM.Ext.vex.GS_DISK.TotalSectors0
	TotalTracks	SCCM.Ext.vex.GS_DISK.TotalTracks0
	TracksPerCylinder	SCCM.Ext.vex.GS_DISK.TracksPerCylinder0

Microsoft.Windows.Peripherals.Processor

The following table describes the mappings for the **Microsoft.Windows.Peripherals.Processor** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_PROCESSOR.Name0
Microsoft.Windows.LogicalDevice	DeviceID [Key]	SCCM.Ext.vex_GS_PROCESSOR.DeviceID0
	Name	SCCM.Ext.vex_GS_PROCESSOR.Name0
	Description	SCCM.Ext.vex.GS_PROCESSOR.Name0
Microsoft.Windows.Processor	Family	SCCM.Ext.vex.GS_PROCESSOR.Family0
	MaxClockSpeed	SCCM.Ext.vex.GS_PROCESSOR.MaxClockSpeed0
	Type	SCCM.Ext.vex.GS_PROCESSOR.ProcessorType0
	BrandID	SCCM.Ext.vex.GS_PROCESSOR.BrandID0
	PCache	SCCM.Ext.vex.GS_PROCESSOR.PCache0
	CPUKey	SCCM.Ext.vex.GS_PROCESSOR.CPUKey0
	IsMobile (bool)	SCCM.Ext.vex.GS_PROCESSOR.IsMobile0
	IsMultiCore (bool)	SCCM.Ext.vex.GS_PROCESSOR.IsMulticore0
Microsoft.Windows.Peripherals.Processor	Manufacturer	SCCM.Ext.vex.GS_PROCESSOR.Manufacturer0
	Speed	SCCM.Ext.vex.GS_PROCESSOR.NormSpeed0
	DataWidth	SCCM.Ext.vex.GS_PROCESSOR.DataWidth0
	Revision	SCCM.Ext.vex.GS_PROCESSOR.Revision0
	Version	SCCM.Ext.vex.GS_PROCESSOR.Version0

Microsoft.Windows.Peripherals.NetworkAdapter

The following table describes the mappings for the **Microsoft.Windows.Peripherals.NetworkAdapter** type.

Service Manager type	Service Manager property	Column name of Configuration Manager Database Views
System.Entity	DisplayName	SCCM.Ext.vex_GS_NETWORK_ADAPTER.Name0
Microsoft.Windows.LogicalDevice	DeviceID [Key]	SCCM.Ext.vex_GS_NETWORK_ADAPTER.DeviceID0
	Name	SCCM.Ext.vex_GS_NETWORK_ADAPTER.Name0
	Description	SCCM.Ext.vex.GS_NETWORK_ADAPTER.Description0
Microsoft.Windows.NetworkAdapter	Bandwidth	SCCM.Ext.vex.GS_NETWORK_ADAPTER.Speed0
	MaxSpeed (int)	SCCM.Ext.vex.GS_NETWORK_ADAPTER.MaxSpeed0
	ProductName	SCCM.Ext.vex.GS_NETWORK_ADAPTER.ProductName0
	DefaultIPGateway	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.DefaultIPGateway0
	DHCPHostName	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.DHCPServer
	IPEnabled	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.IPEnabled0
Microsoft.Windows.Peripherals.NetworkAdapter	AdapterType	SCCM.Ext.vex.GS_NETWORK_ADAPTER.AdapterType0
	Index	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.Index0
	Manufacturer	SCCM.Ext.vex.GS_NETWORK_ADAPTER.Manufacturer0
	MACAddress	SCCM.Ext.vex.GS_NETWORK_ADAPTER.MACAddress0

Service Manager type	Service Manager property	Column name of Configuration Manager Database Views
	ServiceName	SCCM.Ext.vex.GS_NETWORK_ADAPTER.ServiceName0
	DHCPEnabled	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.DHCPEnabled0
	DHCPServer	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.DHCPServer0
	DNSDomain	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.DNSDomain0
	IPAddress	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.IPAddress0
	IPSubnet	SCCM.Ext.vex.GS_NETWORK_ADAPTER_CONFIGUR.IPSubnet0

System.DeviceHasSoftwareItemInstalled

The following table describes the mappings for the **System.DeviceHasSoftwareItemInstalled** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.Entity	DisplayName	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.ProductName0
System.SoftwareItem	ProductName [Key]	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.ProductName0
	Publisher [Key]	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.Publisher0
	VersionString [Key]	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.ProductVersion0
	MajorVersion	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.VersionMajor0
	MinorVersion	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.VersionMinor0

Service Manager type	Service Manager property	Column name of Configuration Manager database views
	LocaleID	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.Language0
System.DeviceHasSoftwareItemInstalled	InstalledDate	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.InstalledDate0
	InstalledPath	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.InstalledLocation0
	SerialNumber	SCCM.Ext.vex_GS_INSTALLED_SOFTWARE.ProductID0
	IsVirtualApplication	SCCM.Ext.Vex_GS_INSTALLED_SOFTWARE.InstallType

System.DeviceHasSoftwareUpdateInstalled

The following table describes the mappings for the **System.DeviceHasSoftwareUpdateInstalled** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.SoftwareUpdate	Vendor [Key]	SCCM.Ext.vex_LocalizedCategoryInstances.CategoryInstanceName
	Title [Key]	SCCM.Ext.vex_LocalizedCIProperties.DisplayName
Microsoft.Windows.SoftwareUpdate	ArticleID	SCCM.Ext.vex_UpdateCIs.ArticleID
	BulletinID	SCCM.Ext.vex_UpdateCIs.BulletinID
	SupportString	SCCM.Ext.vex_LocalizedCIProperties.CIInformativeURL
	Classification	SCCM.Ext.vex_LocalizedCategoryInstances.CategoryInstanceName
System.DeviceHasSoftwareUpdateInstalled	InstallStatus	SCCM.Ext.vex_UpdateComplianceStatus.Status

Microsoft.SystemCenter.ConfigurationManager.DCM_CI

The following table describes the mappings for the **Microsoft.SystemCenter.ConfigurationManager.DCM_CI** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
Microsoft.SystemCenter.ConfigurationManager.DCM_CI	DisplayName	SCCM.Ext.vex_LocalizedCIProperties.DisplayName
	UniqueID [Key]	SCCM.Ext.vex_ConfigurationItems.CI_UniqueID
	Description	SCCM.Ext.vex_LocalizedCIProperties.Description
	IsBaseline	SCCM.Ext.vex_ConfigurationItems.CIType_ID

Microsoft.SystemCenter.ConfigurationManager.DCM_NoncompliantCI

The following table describes the mappings for the **Microsoft.SystemCenter.ConfigurationManager.DCM_NoncompliantCI** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
Microsoft.SystemCenter.ConfigurationManager.DCM_NoncompliantCI	UniqueID [Key]	SCCM.Ext.vex_ConfigurationItems.CI_UniqueID
	Baseline_UniqueID [Key]	SCCM.Ext.vex_ConfigurationItems.CI_UniqueID
	MaxNonComplianceCriticality [Key]	SCCM.Ext.vex_CICurrentComplianceStatus.MaxNoncomplianceCriticality

System.Domain.User

The following table describes the mappings for the **System.Domain.User** type.

Configuration Manager class	Configuration Manager database value	Service Manager property
System.Domain.User	Domain [Key]	Parse SCCM_Ext.vex_GS_SYSTEM_CONSOLE_USER
	UserName [Key]	Parse SCCM_Ext.vex_GS_SYSTEM_CONSOLE_USER

Microsoft.SystemCenter.ConfigurationManagergr.CollectionInf

The following table describes the mapping for the **Microsoft.SystemCenter.ConfigurationManagergr.CollectionInf** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.ConfigItem	DisplayName	SCCM_Ext.vex_Collection.CollectionName
Microsoft.SystemCenter.ConfigurationManagergr.CollectionInf	Count	Count of computers in collection
	CollID [Key]	SCCM_Ext.vex_Collection.CollID
	CollectionName	SCCM_Ext.vex_Collection.CollectionName
	CollectionID	SCCM_Ext.vex_Collection.CollectionID

Microsoft.ConfigMgr.SoftwarePackage

The following table describes the mapping for the **Microsoft.ConfigMgr.SoftwarePackage** type.

Service Manager type	Service Manager property	Column name of Configuration Manager database views
System.ConfigItem	DisplayName	SCCM_Ext.vex_Package.Name
Microsoft.ConfigMgr.SoftwarePackage	ID [Key]	SCCM_Ext.vex_Package.PackageID
	Version	SCCM_Ext.vex_Package.Version

Service Manager type	Service Manager property	Column name of Configuration Manager database views
	Language	SCCM_Ext.vex_Package.Language
	Manufacturer	SCCM_Ext.vex_Package.Manufacturer
	Description	SCCM_Ext.vex_Package.Description

Appendix D - System Center 2012 - Service Manager Registry Keys

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.

System Center 2012 – Service Manager stores many settings in the registry. You seldom have to edit the registry yourself, because most of those settings are derived from entries that you make in day-to-day use. However, some changes to settings might occasionally be required. Service Manager stores most registry values in the following locations:

- HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center\2010

Service Manager Console Registry Keys

The keys in this section are used to manage the Service Manager console for the Service Manager console user. These keys are found in the HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console directory.

Key	Description and value
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleDisplaySettings\NavigationPaneExpanded	The navigation pane is expanded when the value is set to 1 and not expanded when the value is set to 0.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleDisplaySettings\NavigationPaneWidth	Specifies the navigation pane width, limited to display resolution.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service	The **Tasks** pane is expanded when the value is set to 1, and not expanded when the value

Key	Description and value
Manager\Console\ConsoleDisplaySettings\TasksPaneExpanded	is set to 0.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleDisplaySettings\NaN	Specifies the **Tasks** pane width, limited to display resolution.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleDisplaySettings\ForceHighContrast	High Contrast is enabled when the value is set to 1, and not enabled when the value is set to 0.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleWindowSettings\IsConsoleMaximized	The Service Manager console is maximized when the value is set to 1, and not maximized when the value is set to 0.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleWindowSettings\ConsoleLocation\X	Specifies the top left corner of the Service Manager console horizontal coordinate.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleWindowSettings\ConsoleLocation\Y	Specifies the bottom left corner of the Service Manager console vertical coordinate.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleWindowSettings\ConsoleSize\Height	Specifies the height of the Service Manager console, limited to display resolution.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ConsoleWindowSettings\ConsoleSize\Width	Specifies the width of the Service Manager console, limited to display resolution.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\SmConsoleDisplaySettings\NavigationPaneVisible	The Service Manager console navigation pane is visible when the value is set to 1 and hidden when the value is set to 0.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\SmConsoleDisplaySettings\TasksPaneVisible	The Service Manager console **Tasks** pane is visible when set to 1 and hidden when the value is set to 0.

Key	Description and value
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\SmConsoleDisplaySettings\SelectedWunderBarIndex	Depending on the value, the corresponding workspace is selected in the Service Manager console. **Administration** = 0, **Library** = 1, **Work Items** = 2, **Configuration Items** = 3, **Data Warehouse** = 4, **Reporting** = 5. Values higher than 5 correspond to any custom workspaces that are added to the Service Manager console.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\SmConsoleDisplaySettings\NavigationModelNodeLocation	The value for the key is the last view that the user selected before closing the Service Manager console, so that when the Service Manager console reopens, it reopens in this view. **msscnav://root/Windows/Window/ConsoleDisplay/Folder.f837da16-dc5d-7a25-1b48-c62eb5965806/Folder.8afcc5db-910c-35a0-700f-fd9a94b4169b/View.fbf52403-7ce7-05c4-0ca9-7c61030e5f57** is an example value.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ViewDisplaySettings\DetailPaneHeight	Specifies the height of the details pane.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\ViewDisplaySettings\DetailPaneExpanded	The Service Manager console details pane is visible when the value is set to 1 and hidden when the value is set to 0.
HKEY_CURRENT_USER\Software\Microsoft\System Center\2010\Service Manager\Console\User Settings\SDKServiceMachine	Specifies the name of the server that the Service Manager console is connected to.

Service Manager Registry Keys

Keys in this section are used to manage functions that are internal to Service Manager.

Key	Description and values
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System	Specifies the group change check

Key	Description and values
Center\2010\Common\GroupCalcPollingIntervalMilliseconds	interval in milliseconds. For more information, see the Planning Guide for System Center 2012 – Service Manager