

System Center Service Manager 2010 SP1 Administrator’s Guide

Microsoft Corporation

Published: December 1, 2010

Authors

Anat Kerry, Bill Anderson, John Downing, and Liza Poggemeyer

Applies To

System Center Service Manager 2010 SP1

Feedback

Send suggestions and comments about this document to [scsmdocs@microsoft.com](mailto:scsmdocs@microsoft.com?subject=Service%20Manager%202010%20SP1%20Administrator's%20Guide).

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

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.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, SQL Server, Windows, 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 |
| December 1, 2010 | Original release of this guide. |

Contents

[System Center Service Manager 2010 SP1 Administrator's Guide 6](#_Toc279066893)

[Using Management Packs in Service Manager 2010 8](#_Toc279066894)

[How to Create a Management Pack File 9](#_Toc279066895)

[How to Export a Management Pack 10](#_Toc279066896)

[How to Import a Management Pack by Using the Service Manager Console 10](#_Toc279066897)

[Using Connectors to Import Data into Service Manager 11](#_Toc279066898)

[Effects of Deleting a Connector on Configuration Items 12](#_Toc279066899)

[Importing Data from Active Directory Domain Services 12](#_Toc279066900)

[About Importing Data from Active Directory Domain Services 13](#_Toc279066901)

[How to Create an Active Directory Connector 14](#_Toc279066902)

[How to Synchronize an Active Directory Connector 15](#_Toc279066903)

[How to Enable and Disable an Active Directory Connector 16](#_Toc279066904)

[How to Import Data from Other Domains 16](#_Toc279066905)

[Importing Data and Alerts from Operations Manager 2007 17](#_Toc279066906)

[How to Import Management Packs for Operations Manager 2007 Configuration Item Connectors 18](#_Toc279066907)

[How to Create an Operations Manager 2007 Connector 19](#_Toc279066908)

[How to Synchronize an Operations Manager 2007 Connector 22](#_Toc279066909)

[How to Disable and Enable an Operations Manager 2007 Connector 23](#_Toc279066910)

[How to Edit an Operations Manager Connector 24](#_Toc279066911)

[Importing Data from Configuration Manager 2007 24](#_Toc279066912)

[About Importing Data from Configuration Manager 2007 25](#_Toc279066913)

[How to Create a Configuration Manager Connector 26](#_Toc279066914)

[How to Disable and Enable a Configuration Manager Connector 28](#_Toc279066915)

[How to Synchronize a Configuration Manager Connector 29](#_Toc279066916)

[How to Configure a Configuration Manager Connector for an Extended SMS\_def.mof File 30](#_Toc279066917)

[Using a CSV File to Import Data into Service Manager 59](#_Toc279066918)

[About Importing Data from Comma-Separated Files into Service Manager 59](#_Toc279066919)

[How to Import Configuration Items from a CSV File 62](#_Toc279066920)

[Configuration Items in Service Manager 62](#_Toc279066921)

[Creating Configuration Items 63](#_Toc279066922)

[About Creating Configuration Items 64](#_Toc279066923)

[How to Manually Create Configuration Items 65](#_Toc279066924)

[How to Create a Service 66](#_Toc279066925)

[How to Create a View for Imported Configuration Items 68](#_Toc279066926)

[Deleting Configuration Items 69](#_Toc279066927)

[How to Initiate the Deletion of a Configuration Item 70](#_Toc279066928)

[How to Complete the Deletion of a Configuration Item 70](#_Toc279066929)

[Managing Configuration Items 71](#_Toc279066930)

[How to Add, View, or Remove Related Configuration Item Information 72](#_Toc279066931)

[Configuring Incident Management in Service Manager 73](#_Toc279066932)

[About Configuring Incident Management in Service Manager 74](#_Toc279066933)

[How to Set File Attachment Limits 76](#_Toc279066934)

[How to Set Incident Priority 77](#_Toc279066935)

[How to Set Resolution Time 77](#_Toc279066936)

[How to Set Operations Manager Web Settings 78](#_Toc279066937)

[How to Create Incident Templates 78](#_Toc279066938)

[How to Configure Your Infrastructure for E-Mail Incident Support 80](#_Toc279066939)

[Configuring Workflows in Service Manager 82](#_Toc279066940)

[How to Configure Incident Workflows 82](#_Toc279066941)

[How to View Workflow Success or Failure 84](#_Toc279066942)

[Configuring Change and Activity Management in Service Manager 84](#_Toc279066943)

[How to Create Change Request Templates 85](#_Toc279066944)

[How to Create a Manual Activity Template 87](#_Toc279066945)

[How to Configure General Change Settings 88](#_Toc279066946)

[How to Configure General Activity Settings 88](#_Toc279066947)

[How to Configure Change Management Workflows 89](#_Toc279066948)

[How to Configure Activity Management Workflows 90](#_Toc279066949)

[Configuring Desired Configuration Management to Generate Incidents in Service Manager 92](#_Toc279066950)

[How to Configure Desired Configuration Management to Generate Incidents 93](#_Toc279066951)

[Configuring Service Manager Notifications 94](#_Toc279066952)

[How to Configure Notification Channels 95](#_Toc279066953)

[How to Create Notification Templates 96](#_Toc279066954)

[How to Subscribe to Notifications 98](#_Toc279066955)

[How to Verify a Notification Configuration 99](#_Toc279066956)

[Using Groups, Queues, and Lists in Service Manager 100](#_Toc279066957)

[About Groups, Queues, and Lists 101](#_Toc279066958)

[How to Create a Group in Service Manager 103](#_Toc279066959)

[How to Create a Queue 104](#_Toc279066960)

[How to Edit a Queue 105](#_Toc279066961)

[How to Add a List Item 105](#_Toc279066962)

[Managing User Roles in Service Manager 106](#_Toc279066963)

[About User Roles 107](#_Toc279066964)

[How to Add a Member to a User Role 110](#_Toc279066965)

[How to Create a User Role 111](#_Toc279066966)

[Managing Run As Accounts 112](#_Toc279066967)

[How to Change the User Credentials for the Operational System Run As Account 113](#_Toc279066968)

[How to Change the Password for the Operational System Run As Account 116](#_Toc279066969)

[How to Change the Workflow Run As Account Credentials 116](#_Toc279066970)

[Managing Knowledge Articles in Service Manager 117](#_Toc279066971)

[How to Create a Knowledge Article 118](#_Toc279066972)

[How to Search for a Knowledge Article 119](#_Toc279066973)

[Using the Service Manager Cmdlets for Windows PowerShell 120](#_Toc279066974)

[Getting Started with Service Manager Cmdlets for Windows PowerShell 120](#_Toc279066975)

[List of the Service Manager Cmdlets 122](#_Toc279066976)

[Managing the Data Warehouse in Service Manager 123](#_Toc279066977)

[About Managing the Data Warehouse 124](#_Toc279066978)

[How to Disable a Data Warehouse Job Schedule 127](#_Toc279066979)

[How to Enable Data Warehouse Job Schedules 128](#_Toc279066980)

[How to View the Status of a Data Warehouse Job 129](#_Toc279066981)

[How to Suspend and Resume a Data Warehouse Job 130](#_Toc279066982)

[How to Schedule a Data Warehouse Job 131](#_Toc279066983)

[How to View Data Warehouse Job History 132](#_Toc279066984)

[How to Troubleshoot a Data Warehouse Job 133](#_Toc279066985)

[Managing the Self-Service Portal 134](#_Toc279066986)

[How to Set the Configuration Manager Configuration 134](#_Toc279066987)

[How to Set End User Portal Contact IT Settings 135](#_Toc279066988)

[How to Configure a Software Deployment Process 136](#_Toc279066989)

[How to Publish Software Packages 137](#_Toc279066990)

[Using Service Manager Tasks to Troubleshoot Computer Problems 138](#_Toc279066991)

[How to Create a Task 138](#_Toc279066992)

[How to Run a Task From an Incident View 140](#_Toc279066993)

[To Configure Service Manager CEIP Settings 140](#_Toc279066994)

[Appendix A - List of User Role Profiles in Service Manager 140](#_Toc279066995)

[Appendix B - Mapping Active Directory Domain Services Attributes to Service Manager Properties 146](#_Toc279066996)

[Appendix C - Mapping Service Manager Properties to Configuration Manager Database Views 150](#_Toc279066997)

[Appendix D - Service Manager Registry Keys 162](#_Toc279066998)

System Center Service Manager 2010 SP1 Administrator's Guide

Welcome to the System Center Service Manager 2010 Administrator’s Guide. 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 company.

In This Section

[Using Management Packs in Service Manager 2010](#ze6591e88afe14bd789f6cd20fe7ef291)

|  |
| --- |
| Provides information about how to create, import, and export management packs in Service Manager. |

[Using Connectors to Import Data into Service Manager](#zb721f761cd214dce8a5d16d296aee7ea)

|  |
| --- |
| Describes how to import data into Service Manager by using connectors. |

[Configuration Items in Service Manager](#z56a3eaf0f4df4e5dbfd737a6e8ff702b)

|  |
| --- |
| Describes how to manage configuration items in Service Manager. |

[Configuring Incident Management in Service Manager](#z500513e5a7b44e1782f4d4a61775a616)

|  |
| --- |
| Describes how to set configuration settings that streamline the creation of incidents in Service Manager. |

[Configuring Workflows in Service Manager](#z5e81d778674a45cc89d88606047904f8)

|  |
| --- |
| Describes how to create and use workflows in Service Manager. |

[Configuring Change and Activity Management in Service Manager](#zfc36b34fc8fa45708913931d770a61a3)

|  |
| --- |
| Describes how to streamline change and activity management in Service Manager. |

[Configuring Desired Configuration Management to Generate Incidents in Service Manager](#z13aff1a012b64cff8192cdef953938cb)

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

[Configuring Service Manager Notifications](#z0a235c3fa70648789d6d12a14e4dd440)

|  |
| --- |
| Describes how to configure notifications in Service Manager. |

[Using Groups, Queues, and Lists in Service Manager](#z816dadcaa1e042aab284bc8a3bf0575f)

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

[Managing User Roles in Service Manager](#z96a45fee05be4b9d853e843f94e10d94)

|  |
| --- |
| 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](#z42d6137694184ff8922b26e7cb1cbfca)

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

[Managing Knowledge Articles in Service Manager](#zbff2cb4a0a30487cb197105dfe507c8f)

|  |
| --- |
| Describes how to create and search for knowledge articles. |

[Using the Service Manager Cmdlets for Windows PowerShell](#zd4edbfbab9624e339bb7a5fc2376c2b0)

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

[Managing the Data Warehouse in Service Manager](#z3227f7e83cc14444aa4d8077f27f3c2d)

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

[Managing the Self-Service Portal](#z1ea0b1d611c647dda90194849b9e61af)

|  |
| --- |
| Describes how to set the Configuration Manager configuration, publish contact information, configure the software deployment process, and how to publish software packages in the Self-Service Portal. |

[Using Service Manager Tasks to Troubleshoot Computer Problems](#z22e607676e6047cd9a303434e6c61c69)

|  |
| --- |
| Describes how to use tasks to troubleshoot computer problems. |

[To Configure Service Manager CEIP Settings](#ze137fde1452849e09232c8bd4983a81c)

|  |
| --- |
| Describes how to configure CEIP settings in Service Manager. |

[Appendix A - List of User Role Profiles in Service Manager](#z6cd6943652ab4d7aa3a30d33187b7d88)

|  |
| --- |
| Lists the user role profiles. |

[Appendix B - Mapping Active Directory Domain Services Attributes to Service Manager Properties](#zca028b1127ca4299974fe6c2e7265f54)

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

[Appendix C - Mapping Service Manager Properties to Configuration Manager Database Views](#z31290f89862f4fb8b2d402504d072dd1)

|  |
| --- |
| Describes the mapping of data that is imported by Configuration Manager Connector to Service Manager properties. |

[Appendix D - Service Manager Registry Keys](#zf3a041961f33484397d3dd267a35a4a9)

|  |
| --- |
| Describes registry settings for System Center Service Manager 2010. |

Using Management Packs in Service Manager 2010

Management packs are used to extend System Center Service Manager 2010 with the information that you must have to implement all or part of a service management process. You can use 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 a management pack. Then, you can export that management pack to a file and then import the file to another environment, such as a production environment.

A 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. 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.

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. Typically, the management pack is stored in an .xml file that you can import by using the Service Manager console.

In This Section

[How to Create a Management Pack File](#zef914baf911b44ef866e7006631bf1f1)

|  |
| --- |
| Describes how to create a management pack file. |

[How to Export a Management Pack](#z8effd8898fca4fedbfb387f757c2f914)

|  |
| --- |
| Describes how to export a management pack. |

[How to Import a Management Pack by Using the Service Manager Console](#z8a4bf57b53de491394416dc695e78973)

|  |
| --- |
| Describes how to import a management pack by using the Service Manager console. |

How to Create a Management Pack File

You can use the following procedure to create a management pack file. 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 the topic [Management Packs: How to Work with Management Packs](http://go.microsoft.com/fwlink/?LinkId=207159) (http://go.microsoft.com/fwlink/?LinkId=207159).

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. |

How to Export a Management Pack

After you create a management pack, you can export it to a file to back up any customizations in the management pack. After you export a management pack, you can later import it to restore the objects that the management pack contains. You can only export unsealed management packs using the Service Manager console. You must use Windows PowerShell commands to export sealed management packs. For more information about Windows PowerShell commands in Service Manager, see [Using the Service Manager Cmdlets for Windows PowerShell](#zd4edbfbab9624e339bb7a5fc2376c2b0).

You can use the following procedure to export a management pack.

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. |

How to Import a Management Pack by Using the Service Manager Console

Before you can use a management pack in System Center Service Manager 2010, 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](http://go.microsoft.com/fwlink/?LinkId=201286) (http://go.microsoft.com/fwlink/?LinkId=201286) on TechNet.

When you import a management pack that was previously imported, the objects in the management pack overwrite the existing objects. Before you import a management pack that has dependent management packs, you must import the dependent management packs. Alternatively, you can import the management pack and its dependent management packs at the same time, but the dependent management packs must be in the correct order.

Use the following procedure to import a single management pack, or a bundled management pack (.mpb file name extension) by using the Service Manager console.

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. |

Using Connectors to Import Data into Service Manager

Service Manager connectors let you import data as configuration items from Active Directory Domain Services (AD DS), System Center Configuration Manager, and Operations Manager 2007. In addition, you can import alerts from Operations Manager 2007, and these alerts can be configured to automatically generate incidents in Service Manager. You can also import data from comma-separated value files into the Service Manager database.

In This Section

[Effects of Deleting a Connector on Configuration Items](#z804fcbf7fdd34990bcab8d03dd57e4c8)

|  |
| --- |
| Describes the effects of deleting a connector. |

[Importing Data from Active Directory Domain Services](#zc4a1eb3d767c459dabb46f89af8948f0)

|  |
| --- |
| Describes how to create, synchronize, and disable or enable an Active Directory connector. |

[Importing Data and Alerts from Operations Manager 2007](#z5793c18edff6437db8febfee9b66fac8)

|  |
| --- |
| Describes how to create synchronize, edit, and disable or enable an Operations Manager 2007 alert or configuration item (CI) connector. |

[Importing Data from Configuration Manager 2007](#zb6d0e809c56d4668948ccf4f23dd94e3)

|  |
| --- |
| 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. |

[Using a CSV File to Import Data into Service Manager](#z205ee9c181f14a7ebe4e10587ee80fbc)

|  |
| --- |
| Describes how to import data into System Center Service Manager 2010 by using a comma-separated value (CSV) file. |

Effects of Deleting a Connector on Configuration Items

Many of the configuration items that are found in the Service Manager database are the result of the data imported by using connectors. Therefore, if a connector is deleted, the configuration items 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.

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 Service Manager 2010. This section also describes how to create, synchronize, and enable or disable an Active Directory connector.

In This Section

[About Importing Data from Active Directory Domain Services](#zfa5b85ff57dd4c938ef6e0e6a848b8db)

|  |
| --- |
| Provides an overview of how to use a connector to import data from AD DS. |

[How to Create an Active Directory Connector](#z0cf31209b0694762bbad95aac69d352d)

|  |
| --- |
| Describes how to create an Active Directory connector. |

[How to Synchronize an Active Directory Connector](#za33fb75cdbe64772988b8cfb2f670b70)

|  |
| --- |
| Describes how to synchronize the data in AD DS with the Service Manager database. |

[How to Enable and Disable an Active Directory Connector](#zdc595a2795ff42199cfd9526647f0374)

|  |
| --- |
| Describes how to enable or disable an Active Directory connector. |

[How to Import Data from Other Domains](#zb40f988677ed460d9b99893d491466e8)

|  |
| --- |
| Describes how to import data from domains other than the domain in which System Center Service Manager 2010 resides. |

About Importing Data from Active Directory Domain Services

The System Center Service Manager 2010 database contains information about your enterprise and 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 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.

The users you import from Active Directory Domain Services (AD DS) can later be assigned to a user role, so that specific permissions are granted to specific users. However, users who do not exist in your organization’s Active Directory may need to be assigned to an activity. In this case, you must manually create a configuration item that contains all the necessary information about these users.

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 Active Directory Domain Services 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 1.5 to 2 hours. 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](#z0cf31209b0694762bbad95aac69d352d)

[How to Enable and Disable an Active Directory Connector](#zdc595a2795ff42199cfd9526647f0374)

[How to Synchronize an Active Directory Connector](#za33fb75cdbe64772988b8cfb2f670b70)

[How to Import Data from Other Domains](#zb40f988677ed460d9b99893d491466e8)

[Appendix B - Mapping Active Directory Domain Services Attributes to Service Manager Properties](#zca028b1127ca4299974fe6c2e7265f54)

How to Create an Active Directory Connector

You can use the following procedure in System Center Service Manager 2010 to create 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. Follow 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 Next.  Note  Special characters (such as the ampersand [&]) in the User Name box are not supported.  f. On the Select objects page, select All computers, printers, users, and user groups to import all items. Or, select Select individual computers, printers, users or user groups to import only the selected items. 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 following confirmation message:  Active Directory connector successfully configured.  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. |

How to Synchronize an Active Directory Connector

To ensure that the System Center Service Manager 2010 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.

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 Enable and Disable an Active Directory Connector

You can use the following procedure to disable or enable an Active Directory connector.

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. |

To validate the status change of an Active Directory connector

|  |
| --- |
| 1. 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. |

How to Import Data from Other Domains

You can import data from domains other than the domain in which System Center Service Manager 2010 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:   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.   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 organizational unit 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 Operations Manager 2007

If your organization uses System Center Operations Manager 2007 to monitor systems in your enterprise, the agents that are deployed gather information about configuration items that are discovered and, as problems are detected, Operations Manager 2007 generates alerts. Two connectors for Operations Manager are available in System Center Service Manager 2010: 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.

Operations Manager 2007 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 Operations Manager 2007 management packs. Therefore, you must import some Operations Manager 2007 management packs into Service Manager. When you install Service Manager, a set of Operations Manager 2007 management packs for common objects and the required Windows PowerShell script are copied to your Service Manager installation folder. For more information, see [How to Import Management Packs for Operations Manager 2007 Configuration Item Connectors](#zcd08e205d4364595b2f97293637a74e9). 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 an Operations Manager Connector](#z6478f7b377414825866debe9a2923013).

In This Section

[How to Import Management Packs for Operations Manager 2007 Configuration Item Connectors](#zcd08e205d4364595b2f97293637a74e9)

|  |
| --- |
| Describes how to import the management packs necessary for the Operations Manager 2007 configuration item connectors. |

[How to Create an Operations Manager 2007 Connector](#zd52c21465a2e4e67bd3813883d1d42c8)

|  |
| --- |
| Describes how to create an Operations Manager 2007 connector and import configuration items and alerts from Operations Manager 2007. |

[How to Synchronize an Operations Manager 2007 Connector](#z8389b323617f47079f92df3e91836ec0)

|  |
| --- |
| Describes how to synchronize an Operations Manager 2007 connector to reflect changes that you made in Operations Manager. |

[How to Disable and Enable an Operations Manager 2007 Connector](#z9bac99b341a04fb3a8209e34373c2b3e)

|  |
| --- |
| Describes how to disable and enable an Operations Manager 2007 connector to pause or resume data synchronization. |

[How to Edit an Operations Manager Connector](#z6478f7b377414825866debe9a2923013)

|  |
| --- |
| Describes how to edit properties for an Operations Manager connector. |

How to Import Management Packs for Operations Manager 2007 Configuration Item Connectors

For the System Center Operations Manager 2007 configuration item (CI) connector to function correctly, you have to import a set of management packs into System Center Service Manager 2010. 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 2010\Operations Manager Management Packs. Use the following procedure to import the management packs into Service Manager.

To import management packs for the Operations Manager 2007 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.  Set-ExecutionPolicy Unrestricted  Set-Location \"Program Files\Microsoft System Center\Service Manager 2010\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 |

How to Create an Operations Manager 2007 Connector

In System Center Service Manager 2010, there are two types of connectors for System Center Operations Manager 2007. 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.

Note

For the System Center Operations Manager 2007 configuration item (CI) connector to function correctly, you have to import a set of management packs into System Center Service Manager 2010. For more information, see [How to Import Management Packs for Operations Manager 2007 Configuration Item Connectors](#zcd08e205d4364595b2f97293637a74e9) .

Alerts that are generated by Operations Manager 2007 and that are sent to Service Manager do not contain user information. Therefore, when you open the 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](#z21674b6180264997b7f4b6938fe0a004). 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 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 2007 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. Follow these 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 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](http://go.microsoft.com/fwlink/?LinkId=207215) (http://go.microsoft.com/fwlink/?LinkId=182907) in the System Center Service Manager 2010 SP1 Planning Guide.  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 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, and connect to the Operations Manager root management server.  6. Use the appropriate method based on the version of Operations Manager 2007 you are using:   In Operations Manager 2007 SP1, in the Administration pane, click Product Connectors.   In Operations Manager 2007 R2, in the Administration pane, click Product Connectors, and then click Internal Connectors.  7. In the Connectors pane, click the name of the alert connector 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 2007 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 2007 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. Follow these 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:   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](http://go.microsoft.com/fwlink/?LinkId=198071) (http://go.microsoft.com/fwlink/?LinkId=198071) in the System Center Service Manager Deployment Guide.  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 2007 CI connector

|  |
| --- |
|  Confirm that objects discovered by Operations Manager are listed as configuration items in Service Manager. |

To confirm the status of an Operations Manager 2007 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. |

How to Synchronize an Operations Manager 2007 Connector

When you create a System Center Operations Manager alert connector for System Center Service Manager 2010, 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 an Operations Manager 2007 Connector

You can use the following procedure to disable or enable a System Center Operations Manager connector for System Center Service Manager 2010.

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 Operations Manager 2007, see [Removing an Old Product Connector](http://go.microsoft.com/fwlink/?LinkId=188974) (http://go.microsoft.com/fwlink/?LinkId=188974) on Kevin Holman’s Operations Manager 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. |

How to Edit an Operations Manager Connector

After you install a System Center Operations Manager 2007 alert connector and 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 Configuration Manager 2007

This section provides an overview of how to use a connector to import data from System Center Configuration Manager into System Center Service Manager 2010. 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.

In This Section

[About Importing Data from Configuration Manager 2007](#z2f3804eefe4f40bfb510fc3eb1d970f8)

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

[How to Create a Configuration Manager Connector](#z4a62db4876fc416da0f145e97d430c42)

|  |
| --- |
| Describes how to create a Configuration Manager connector and import data from Configuration Manager. |

[How to Disable and Enable a Configuration Manager Connector](#zf2a27d23eb254c8c9ce636264edd22c0)

|  |
| --- |
| 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](#zca311f275fad431480e4e6f0602ff9b6)

|  |
| --- |
| 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](#z2d70d3bd03d74a7e9fb1e52519981302)

|  |
| --- |
| Describes how to customize the default Configuration Manager 2007 SMS\_def.mof file to extend the hardware information that is collected. |

About Importing Data from Configuration Manager 2007

You can import data from the Microsoft System Center Configuration Manager 2007 site database into the System Center Service Manager 2010 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 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 can only import data from Microsoft System Center Configuration Manager 2007 with Service Pack 1 or Microsoft System Center Configuration Manager 2007 R2.

Configuration Manager 2007 provides a distributed infrastructure for discovery and collection of hardware and software inventory information, software deployment, software updates, and configuration management. The information that Configuration Manager collects can be imported and then stored in the Service Manager database by using a Configuration Manager Connector. Importing data by using a Configuration Manager Connector can add details about a configuration item that has already been imported by using an Active Directory Connector, or add new configuration items that do not exist in Active Directory domains. You can configure multiple Configuration Manager Connectors to import data from different Configuration Manager site databases.

By using a Configuration Manager Connector, you can import configuration baselines from Configuration Manager and then use them to automatically generate incidents for non-compliant configuration items. For more information about this option, see [How to Configure Desired Configuration Management to Generate Incidents](#z43b098aab8fa4e64a81794357f681e79).

You can configure the Configuration Manager Connector to update the Service Manager database on a recurring schedule. You can also temporarily suspend importing 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.

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](http://go.microsoft.com/fwlink/?LinkId=115631) (http://go.microsoft.com/fwlink/?LinkId=115631).

In System Center Configuration Manager 2007, the hardware inventory can be extended 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](http://go.microsoft.com/fwlink/?LinkID=160640) (http://go.microsoft.com/fwlink/?LinkID=160640).

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.

See Also

How to Configure a Configuration Manager Connector for an Extended SMS\_DEF.MOF File

[How to Create a Configuration Manager Connector](#z4a62db4876fc416da0f145e97d430c42)

[How to Disable and Enable a Configuration Manager Connector](#zf2a27d23eb254c8c9ce636264edd22c0)

[Appendix C - Mapping Service Manager Properties to Configuration Manager Database Views](#z31290f89862f4fb8b2d402504d072dd1)

How to Create a Configuration Manager Connector

You can use the following procedure to create a connector to import data from Microsoft System Center Configuration Manager 2007 with Service Pack 1 into System Center Service Manager 2010.

Important

Before you can create the Configuration Manager connector, you have to verify that 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](http://go.microsoft.com/fwlink/?LinkId=177523) (http://go.microsoft.com/fwlink/?LinkId=177523).

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 Connector Management Pack list, select System Center Configuration Manager 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 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 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 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.  Then, click Close.  Note  The System Center Configuration Manager Connector Wizard may take several hours to import data from 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 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. |

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.

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. 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. |

How to Synchronize a Configuration Manager Connector

To ensure that the System Center Service Manager 2010 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 procedure to manually synchronize the connector.

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

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 which 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 include also 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:

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 importing the management pack, Service Manager processes the directives in the management pack to create staging tables and to run any install 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 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 are logged to the event log. In this case, you must delete the management pack, correct the errors, and re-import 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 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 either 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 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 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 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 to the values in the sample. | Yes |
| IsProvider | In DataProvider template - True  In DataConsumer template - False | Yes |
| SolutionName | A comment. For example, it can indicate the type of the imported data. | Attempt to import a management pack in which the solution name is already being used; 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 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. | 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. |
| DisableParallelProcessing | True |  |
| DataTable Properties |  |  |
| DataName | The table, from which to import data. It is used in the user interface, and not used in queries. |  |
| StageTableName | Name of the staging table. It must be unique. | Attempt to import a management pack, in which the table name is already being used, causes an error logged to the event log. |
| WatermarkField | 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. |
| BatchIdField | Name of 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 | Size of the batch if batching is used. A high number indicates that much data is being read or written at the same time. 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 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 exposed by Configuration Manager 2007 SCCM\_Ext.\* views is supported for import. This data can be extended by using standard sms\_def.mof extensions or by using noidmifs. Other tables are not supported.  Notably subqueries are not supported, but joins to other tables are. | Not validated. All queries have an Lfx\_Status column with value “U” or “D” indicating if the row represents an Update or a Delete operation. |
| CollectionName | A name for a group of data tables – must be unique. Tables in the same collection cannot depend on each other. | Attempt to import a management pack, in which the collection name is already being used, causes an error logged to the event log. |
| PrimaryKeyName | A section that declares the unique primary key name for the staging table. | Attempt to import a management pack, in which key name is already being used, causes an error logged to the event log. |
| DependOnDataTable | Name(s) 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 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 type. Supported types are int, nvarchar, datetime and xml. | Not validated |
| PrimaryKeyACs, PrimaryKeyPosition | If part of primary key, indicates position from 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. | Attempt to import a management pack, in which the collection name is already being used, causes an error logged to the event log. |
| StagingName | In DataProvider template – DefaultCache  In DataConsumer template – Not present | Not validated |
| DataTables | 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 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="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/DataConnectorName$">

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="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/WinFormUIAssembly$">

Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms.SmsConnector,

Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms, Version="7.0.5000.0", Culture=neutral,

PublicKeyToken="31bf3856ad364e35"

</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/InstallSQLScripts$"></Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/DisableParallelProcess$">

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="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/StageTableName$">Sample\_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.[ResourceID]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">2000</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">true</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/GroomType$">2</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CDATA[

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="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">BIOSComputers</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/PrimaryKeyName$">[Sample\_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]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</Property>

</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</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">64</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE\_DEFAULT</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Property>

</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</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">255</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE\_DEFAULT</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Property>

</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="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/StageTableName$">Sample\_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</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">2000</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">true</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/GroomType$">2</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CDATA[

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="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">BIOSComputers</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/PrimaryKeyName$">[Sample\_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]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</Property>

</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]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">1</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</Property>

</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]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">64</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE\_DEFAULT</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Property>

</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]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">32</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE\_DEFAULT</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Property>

</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="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/StageTableName$">Sample\_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.[ResourceID]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">2000</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">true</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/GroomType$">2</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CDATA[

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="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">Sample\_SMS\_PROVIDER\_BIOS\_COLLECTION</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/PrimaryKeyName$">[Sample\_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]</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyPosition$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/PrimaryKeyAcs$">true</Property>

</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</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">false</Property>

</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</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">Int</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Property>

</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</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Type$">NVarChar</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Size$">34</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/Collation$">DATABASE\_DEFAULT</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.Field']/AllowNull$">true</Property>

</Object>

</Object>

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

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollectionName$">BIOSComputers</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/StagingName$">DefaultCache</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">SCCM\_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="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollectionName$">Sample\_SMS\_PROVIDER\_BIOS\_COLLECTION</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/StagingName$">DefaultCache</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">SCCM\_Ext.vex\_GS\_PC\_BIOS</Property>

</Object>

</ObjectTemplate>

<ObjectTemplate ID="DataConsumer.Microsoft.EnterpriseManagement.ServiceManager.Connector.Sms" TypeID="LFX!System.LinkingFramework.DataConnector.Projection">

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/DataConnectorName$">

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.OperationalStoreConsumer

</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="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/InstallSQLScripts$"><![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="$Context/Property[Type='LFX!System.LinkingFramework.DataConnector']/UninstallSQLScripts$"><![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\_SMS\_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.Lfx\_RowId</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">500</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">false</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CDATA[

SELECT \* FROM [LFXSTG].v\_Sample\_SMS\_BIOSComputer E

]]>

</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">Sample\_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\_SMS\_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.Lfx\_RowId</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdType$">0</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/BatchIdSize$">500</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/UseCache$">False</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/QueryString$"><![CDATA[

select C.\* from [LFXSTG].v\_Sample\_BIOS C

]]>

</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataTable']/CollectionName$">Sample\_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="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollectionName$">Sample\_SMS\_Computers\_COLLECTION</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">Sample\_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.Computer</TypeName>

<MPName xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">Microsoft.Windows.Library</MPName>

<MPVersion xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">7.0.5229.0</MPVersion>

<MPToken xmlns="http://schemas.microsoft.com/sdm/servicedesk/linking/2005/09">31bf3856ad364e35</MPToken>

]]>

</Property>

</Object>

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

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataCollectionName$">Sample\_SMS\_BIOS\_CONSUMER\_COLLECTION</Property>

<Property Path="$Context/Property[Type='LFX!System.LinkingFramework.DataCollection']/DataTables$">Sample\_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</TypeName>

<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>

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 Service Manager 2010 by using comma-separated value (CSV) files.

In This Section

[About Importing Data from Comma-Separated Files into Service Manager](#zeca4db47ef1b4afa929b7251f9a8df14)

|  |
| --- |
| Describes the data and format files necessary for importing data from comma-separated files by using the Import from CSV feature. |

[How to Import Configuration Items from a CSV File](#z583eef907e26421ba8a064c6d5178187)

|  |
| --- |
| Describes how to import data items contained in a comma-separated value (CSV) file. |

About Importing Data from Comma-Separated Files into Service Manager

Configuration items contained in a comma-separated values .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. This feature can be used 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](http://go.microsoft.com/fwlink/?LinkId=159957) (http://go.microsoft.com/fwlink/?LinkId=159957) 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](#z583eef907e26421ba8a064c6d5178187)

How to Import Configuration Items from a CSV File

Before you can import data from a comma-separated value (CSV) file, 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](http://go.microsoft.com/fwlink/?LinkId=181443) (http://go.microsoft.com/fwlink/?LinkId=181443). 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 number next to Items saved, Instances created in memory, and Instances committed to database are equal the number of rows in the data file, and then click Close. |

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 Service Manager

Configuration items are a way to store information in the Service Manager database about services, computers, software, software updates, users and other undefined imported objects. You can then select configuration items (CIs) 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 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 [About Importing Data from Configuration Manager 2007](#z2f3804eefe4f40bfb510fc3eb1d970f8) and [About Importing Data from Active Directory Domain Services](#zfa5b85ff57dd4c938ef6e0e6a848b8db).

Note

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

In This Section

[About Creating Configuration Items](#z5158caa2773b46db80de6708407b2cab)

|  |
| --- |
| 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](#ze9e47930f11243b4a70cd7786b46657a)

|  |
| --- |
| Describes the 2-step process required to delete configuration items. |

[Managing Configuration Items](#z3928f87883dc43ecb3d4fe0eeaae9e66)

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

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 Service Manager 2010.

In This Section

[About Creating Configuration Items](#z5158caa2773b46db80de6708407b2cab)

|  |
| --- |
| Provides an overview of how to create configuration items. |

[How to Manually Create Configuration Items](#z21674b6180264997b7f4b6938fe0a004)

|  |
| --- |
| Describes how to manually create computer configuration items. |

[How to Create a Service](#z95e89dbe7ee74999b7d276635afa375c)

|  |
| --- |
| Describes how to manually create a service from configuration items imported from connectors. |

[How to Create a View for Imported Configuration Items](#z49cf2ee075464394b40baa43af32344d)

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

About Creating Configuration Items

Configuration items are a way to store information in the Service Manager database about services, computers, software, software updates, users, and other undefined imported objects. 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, Microsoft System Center Configuration Manager 2007 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 Service Manager](#zb721f761cd214dce8a5d16d296aee7ea).

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 to the System Center Service Manager 2010 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.  c. Click OK.  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 e-mail 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 Service Manager 2010. When you create a service, you create service configuration items, you define their business data, and you define relationships to other configuration items.

You may have to create and define business services that are critical to your enterprise from data in System Center Operations Manager and from configuration items that you manually created. Before you can create a service, you have to create an Operations Manager configuration item (CI) connector so that individual configuration items and distributed applications are automatically imported into System Center Service Manager 2010.

This procedure describes how to import the Active Directory Server Common Library management pack (and any dependencies) into both Operations Manager 2007 and Service Manager. After you import the management pack, make sure that you synchronize the Operations Manager configuration items connector in Service Manager.

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 currently designed to handle a large number of components; as a result, Microsoft recommends that you keep your service map tree structures small.

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 Active Directory Topology Root.  4. In the Tasks pane, under Active Directory Topology Root, click Edit.  5. In the Service Maps – Active Directory Topology Root 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 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 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 Active Directory Topology Root. In the Tasks pane under Active Directory Topology Root, 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 Service Manager 2010 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 you do for other configuration items.  4. Optionally, you can perform actions in the Tasks list, in the same manner 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. |

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. The first step does not delete configuration items directly. Instead, this process changes the property values of a configuration item such 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.

In This Section

[How to Initiate the Deletion of a Configuration Item](#zf9cab2ee084347e8add662c36e241436)

|  |
| --- |
| Describes how to delete a configuration item. |

[How to Complete the Deletion of a Configuration Item](#zaae5165e01ce4722b3b899be3f045f4f)

|  |
| --- |
| Describes how to permanently delete a configuration item. |

How to Initiate the Deletion of a Configuration Item

You can use the following procedure to initiate the deletion of a configuration item in System Center Service Manager 2010. 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. |

See Also

[How to Complete the Deletion of a Configuration Item](#zaae5165e01ce4722b3b899be3f045f4f)

How to Complete the Deletion of 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 Service Manager 2010 administrator can use the following procedure 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 deleted 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. |

See Also

[How to Initiate the Deletion of a Configuration Item](#zf9cab2ee084347e8add662c36e241436)

Managing Configuration Items

You might want to associate the work item to apply the Microsoft Exchange Server with SP1 update to the service that represents the computers that are affected by the e-mail incident. To accomplish this, you can update the service configuration item, and add the respective work item as a related item.

In This Section

[How to Add, View, or Remove Related Configuration Item Information](#zb9f9540993494b2faee94a33dbed9cfb)

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

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. The procedure in this topic describes 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 Service Manager

This section provides an overview of how to configure incident management in System Center Service Manager 2010. This section also contains procedures that cover the three main incident management configuration scenarios: configuring incident settings, creating an incident template, and configuring e-mail incident support.

In This Section

[About Configuring Incident Management in Service Manager](#zd600acd9d3ec487ab9903125522e3c4c)

|  |
| --- |
| Provides an overview of how to configure incident management. |

[How to Set File Attachment Limits](#z2624f3ae54114726b4015d9fcd96730c)

|  |
| --- |
| Describes how to set the number of files and the size of a file that can be attached to an incident. |

[How to Set Incident Priority](#z041f0a40c57d45a09a169a3bc9eb9388)

|  |
| --- |
| Describes how to define the incident priority based on impact and urgency. |

[How to Set Resolution Time](#z402e37d91fec4abe91eba5bb6bd728ab)

|  |
| --- |
| Describes how to define the incident resolution time based on incident priority. |

[How to Set Operations Manager Web Settings](#z21752c1852f4408ea3ce974d899c19be)

|  |
| --- |
| Describes how to specify the URL that Service Manager uses to connect to the Operations Manager 2007 Web console. |

[How to Create Incident Templates](#z869ab262668f43b7ae187dd431466f35)

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

[How to Configure Your Infrastructure for E-Mail Incident Support](#zc892a667856949a8bf2730d5d615063d)

|  |
| --- |
| Describes how to configure Exchange Server and SMTP to let users submit incidents by sending an e-mail. |

About Configuring Incident Management in Service Manager

Several features in System Center Service Manager 2010 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 e-mail-related problems. Help desk personnel use templates when creating incidents. The template pre-populates some of the fields in the incident, such as the name of the support analyst who handles e-mail-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 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 Service Manager 2010, all incident numbers start with "IR". However, you can change the prefix that is used for your incident numbers.

The policy at your company 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



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 from Operations 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 Service Manager 2010 for problems that are, for example, related to e-mail 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 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.

Follow the procedures in this section to create two incident templates; one to create e-mail-related incidents, and another to use with the Incident Change workflow for printer-related problems.

Configuring Incident Support Through E-mail

Instead of placing a call to the help desk, your end-users can submit incidents by sending an e-mail to a dedicated e-mail address. Several e-mail addresses can be used, one for hardware, one for software, and one for printers. For example, when an e-mail 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 e-mail includes an existing server running Exchange Server or SMTP Server and 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 e-mail 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 SMTP domains for incoming and relay e-mail, see [Article 260973](http://go.microsoft.com/fwlink/?LinkId=144911) in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=144911).

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 this example, set the maximum number of files to 5 and the maximum file size to 500 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 Incident Priority

Use the following procedure to define a priority calculation table based on impact and urgency settings 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 1–9, 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.

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 1–9, specify the amount of time for incident resolution.  7. Click OK.  Note  In this release, you must close and then open the Service Manager console before resolutions times are applied to an incident. |

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 procedure to set the Web settings of System Center Operations Manager 2007.

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 Create Incident Templates

Use the following procedures to create two incident templates, the first you use to create e-mail-related incidents and the second you use with the Incident Change workflow for printer-related problems.

To create an e-mail-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, follow 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 e-mail-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, follow 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 E-mail:.  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 e-mail-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, follow 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. |

How to Configure Your Infrastructure for E-Mail Incident Support

Use the following procedures to configure your infrastructure to support the creation of incidents through e-mail.

To configure Exchange 2007 to route e-mails

|  |
| --- |
| 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 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 E-mail 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 e-mails that you want Service Manager to process during an e-mail processing cycle.  8. Select the Turn on incoming e-mails processing check box, and then click OK. |

Configuring Workflows in Service Manager

A workflow is a sequence of activities that automate a business process. Workflows can, for example, update incidents when various changes occur or 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. Workflows activities function by applying templates. For this example, an incident template to change the support tier to a setting of 2 must have been previously created.

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 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. Viewing the log lets you examine the events that occurred when the workflow ran. Viewing the related object presents the form that this workflow acted upon. 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 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.

In This Section

[How to Configure Incident Workflows](#zbcd61675fff246da9000e30843f25470)

|  |
| --- |
| 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](#z63218802c7db4135a73ebfffdc4b4f92)

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

How to Configure Incident Workflows

You can use the following procedure to create 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](#z041f0a40c57d45a09a169a3bc9eb9388) and “To create a new printer-related incident template” in [How to Create Incident Templates](#z869ab262668f43b7ae187dd431466f35).

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, follow 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 incident 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. On the Select People to Notify page, optionally 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. |

How to View Workflow Success or Failure

Use the following procedure to view the success and failure instances of the workflows.

To view workflow success and failures

|  |
| --- |
| 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 All Instances, and then perform 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. |

Configuring Change and Activity Management in Service Manager

As part of your initial Service Manager configuration, 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.

In this scenario, for example, you want all change requests that modify the IT messaging infrastructure to be categorized by functional area.

In This Section

[How to Create Change Request Templates](#z2218b319e5594a7096b54bf13442b489)

|  |
| --- |
| Describes how to construct a change request template to create change requests. |

[How to Create a Manual Activity Template](#z9f3d0517f9584e14898b248243bcb090)

|  |
| --- |
| Describes how to create a manual activity template. |

[How to Configure General Change Settings](#z697e5c1e7a7d4c58ac8dc97bcbff1d4b)

|  |
| --- |
| 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](#zf2e963e98f234b4194cc93362881c8e9)

|  |
| --- |
| Configure settings that are used to specify prefixes for activities. |

[How to Configure Change Management Workflows](#zc7354a9de54e448aa08935fdfb5dd700)

|  |
| --- |
| Describes how to configure change request conditions that can apply a change request template and send notifications. |

[How to Configure Activity Management Workflows](#z55a4ab3bfef846c5ba72a7917e64dc7c)

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

How to Create Change Request Templates

You can use the following procedures to create two change request templates in System Center Service Manager 2010. 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](#zc7354a9de54e448aa08935fdfb5dd700).

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 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

You can use the following procedure to create a manual activity template in System Center Service Manager 2010. 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 need to create a workflow that applies the template. For more information about how to create a workflow, see [How to Configure Incident Workflows](#zbcd61675fff246da9000e30843f25470).

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](#z55a4ab3bfef846c5ba72a7917e64dc7c) 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 procedure in System Center Service Manager 2010 to configure settings to specify change request prefixes and to define change request file attachment limits.

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 Management Settings dialog box. |

To validate change settings

|  |
| --- |
|  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.   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

You can use the following procedure in System Center Service Manager 2010 to configure settings to specify activity prefixes when you view activity records. 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 verify on the Activities tab that activities have the new prefix that you specified. |

How to Configure Change Management Workflows

You can use the following procedure in System Center Service Manager 2010 to set the priority of all standard change requests. 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 follow the steps in this procedure, you have to create the following templates:

 Set Standard Change Requests to Low Priority: For more information, see the "To create a priority-modifying template" procedure in the [How to Create Change Request Templates](#z2218b319e5594a7096b54bf13442b489) topic.

 New Standard Change Request Received Template: For more information, see the "To create a notification template for change requests" procedure in the [How to Create Notification Templates](#zfd4ac55db0b74101ac97819a491b23af) topic.

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 list, select When a new object of class Change Request 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 Send notifications for this workflow rule 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 e-mail is sent to the user who created the change request. |

How to Configure Activity Management Workflows

You can use the following procedure in System Center Service Manager 2010 to automatically assign all unassigned manual activities to a named user.

Before you can follow 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](#z9f3d0517f9584e14898b248243bcb090).

 New Activity Assigned Received Template: For more information, see [How to Create Notification Templates](#zfd4ac55db0b74101ac97819a491b23af).

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 e-mail 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 a new object of class Manual Activity 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 Send notifications for this workflow rule check box.  18. In the Templates list, select New Activity Assigned Received Template, click Add, and then click Next.  19. On the Summary page, click Create.  20. On the Completion page, click Close.  21. 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 Desired Configuration Management to Generate Incidents in 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 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](http://go.microsoft.com/fwlink/?LinkId=133540) (http://go.microsoft.com/fwlink/?LinkId=133540).

In 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 the [About Importing Data from Configuration Manager 2007](#z2f3804eefe4f40bfb510fc3eb1d970f8).

Desired configuration management in Configuration Manager 2007 lets you 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.

In This Section

[How to Configure Desired Configuration Management to Generate Incidents](#z43b098aab8fa4e64a81794357f681e79)

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

How to Configure Desired Configuration Management to Generate Incidents

In System Center Service Manager 2010, 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.

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, follow 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. Then, 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. |

Configuring Service Manager Notifications

You may want to be notified when incidents or other changes occur. 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 e-mail 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 will need to 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 in order for notifications to function properly. See the topic “How to Add a Member to a User Role” in the [System Center Service Manager Administrator’s Guide](http://go.microsoft.com/fwlink/?LinkId=178233) at http://go.microsoft.com/fwlink/?LinkId=178233

In This Section

[How to Configure Notification Channels](#zf1d9cbd9b3fe4845bc9cd57da5c9324c)

|  |
| --- |
| Describes how to set up a notification channel. |

[How to Create Notification Templates](#zfd4ac55db0b74101ac97819a491b23af)

|  |
| --- |
| Describes how to set up a notification template. |

[How to Subscribe to Notifications](#z910f5e7674824a02a3846c622d12468e)

|  |
| --- |
| Describes how to subscribe to a notification for you or for others. |

[How to Verify a Notification Configuration](#z97da0e3bccb44e92883ec5a8bd9397ba)

|  |
| --- |
| Describes how to verify that notification configuration is set up correctly. |

How to Configure Notification Channels

You can use the following procedure to configure notification channels in System Center Service Manager 2010. 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 e-mail notifications that are sent by Service Manager to a Simple Mail Transfer Protocol (SMTP) server.

Note

In this release of Service Manager, only e-mail notification is supported.

To configure e-mail 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 Configure 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 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 e-mail address of the service account 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 e-mail notifications. For example, select 25.  11. Click OK to close the dialog box. |

To validate e-mail 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. Verify that the configuration you entered is correct. |

How to Create Notification Templates

You can use the following procedures in System Center Service Manager 2010 to create notification templates for incidents, change requests, and newly assigned activities. After you create the notification templates, you can use a notification subscription to send e-mail messages based on the templates. The notification template determines the type and format of the message to send.

Note

Manually copying and pasting substitution strings from other notification templates will not generally work so you should avoid copying them to prevent errors.

Two of the following procedures are prerequisites for other topics:

 The New Activity Assigned Received Template described in the procedure To create a notification template for a newly assigned activity is the template you will need for the procedure [How to Configure Activity Management Workflows](#z55a4ab3bfef846c5ba72a7917e64dc7c).

 The New Standard Change Request Received Template described in the procedure To create a notification template for change requests is the template you will need for the procedure [How to Configure Change Management Workflows](#zc7354a9de54e448aa08935fdfb5dd700).

Note

In this release of Service Manager, notifications are sent only by e-mail.

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 the Service Manager Incident Management Configuration Library management pack is selected, and then click Next.  8. On the Template Design page, in the Message subject box, type a subject for the e-mail 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 e-mail 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 the Service Manager Change Management Configuration Library management pack is selected, and then click Next.  8. On the Template Design page, in the Message subject box, type a subject for the e-mail 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 the Service Manager Activity Management Configuration Library management pack is selected, and then click Next.  8. On the Template Design page, in the Message subject box, type a subject for the e-mail template. For example, type New Activity Assigned with ID#. Then, click Insert.  9. In the Select Property dialog box, select Sequence 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. |

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 Service Manager 2010 to subscribe to notifications by using the Notification Subscription wizard. Then, notifications will be sent when an object is created, updated, or deleted.

In this procedure, you set up a subscription so that a messaging analyst is notified when a new incident that pertains to an e-mail problem is opened.

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 and the settings do not change.

To create a notification subscription

|  |
| --- |
| 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 Choose Class dialog box, choose a class. For example, click Incident. Then, click OK.  8. In the When to notify box, select When an object of the selected class is created.  9. Make sure that the Service Manager Incident Management Configuration Library management pack is selected, and then click Next.  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 Summary page, review the settings that you selected for the notification subscription, and then click Create.  17. On the Completion page, click Close. |

To validate the notification subscription

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

See Also

[How to Configure Notification Channels](#zf1d9cbd9b3fe4845bc9cd57da5c9324c)

[How to Create Notification Templates](#zfd4ac55db0b74101ac97819a491b23af)

How to Verify a Notification Configuration

You can use the following procedure in System Center Service Manager 2010 to verify that you have correctly configured notifications. Generate the type of change that activates the notification subscription that was previously created. By doing this, the subscription generates and then sends a notification. Receipt of the notification verifies success. For example, create a test incident that generates an e-mail notification. The notification informs the recipient that an incident was opened.

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 e-mail notification that contains the information you entered in the template is received. The e-mail title should contain the incident ID number. |

Using Groups, Queues, and Lists in Service Manager

In 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 following procedures to help you manage these items.

In This Section

[About Groups, Queues, and Lists](#z3b3748d9a1a1437394f7a60be81ade3e)

|  |
| --- |
| Provides an overview of groups, queues, and lists in Service Manager. |

[How to Create a Group in Service Manager](#za61ef0961fb34a1692d97814baf15ebc)

|  |
| --- |
| Describes how to create a group. |

[How to Create a Queue](#z8feecb898fce4b33bd890c3732765102)

|  |
| --- |
| Describes how to create a queue. |

[How to Edit a Queue](#z7d9bbf6a3bf34b788eeb4df8dadf19cd)

|  |
| --- |
| Describes how to edit a queue. |

[How to Add a List Item](#z418a72b4e5884b40bd584d5089f0a195)

|  |
| --- |
| Describes how to add a list item. |

About Groups, Queues, and Lists

The Library pane 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 System Center Service Manager 2010, 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, 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. 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 inclusion rule samples.

|  |  |  |
| --- | --- | --- |
| 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, 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. 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 configuring 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 such as 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 ticket. Queues use membership rules to determine which work items should be included in the queue. Queues membership rules are dynamic and 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, a queue can be used as criteria in a subscription to specify which work items to notify about.

 In security, a queue can be used 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 contained in the queue are preserved. You can only delete a queue that is in an unsealed management pack.

Using Lists to Customize Forms

Lists in System Center Service Manager 2010 let you 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 the property.

Lists are used in forms and dialog boxes throughout the Service Manager console. Lists and list items let users 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 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 in Service Manager](#za61ef0961fb34a1692d97814baf15ebc)

[How to Create a Queue](#z8feecb898fce4b33bd890c3732765102)

[How to Edit a Queue](#z7d9bbf6a3bf34b788eeb4df8dadf19cd)

[How to Add a List Item](#z418a72b4e5884b40bd584d5089f0a195)

How to Create a Group in Service Manager

Use the following procedure 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 example. For more information, see [Importing Data from Configuration Manager 2007](http://go.microsoft.com/fwlink/?LinkId=181512) (http://go.microsoft.com/fwlink/?LinkId=181512).

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 Connector Configuration Management Pack. 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 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 are displayed in the Group Members window. |

How to Create a Queue

System Center Service Manager 2010 includes several predefined queues. Additionally, you can create queues if your organization requires custom queues. For example, you can create an escalation queue 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. Follow 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, 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. |

How to Edit a Queue

In System Center Service Manager 2010, 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 Service Manager 2010, you can use this procedure to add a list item to an existing list. 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 “How to Manually Create a New Incident” topic in the System Center Service Manager 2010 Operations Guide. |

Managing User Roles in Service Manager

This section provides an overview of user roles in System Center Service Manager 2010 and includes procedures that you can use to work with user roles.

In This Section

[About User Roles](#z981d4754b80e44658a79306307fd5a9c)

|  |
| --- |
| Provides an overview of user roles. |

[How to Add a Member to a User Role](#z3df2547120944e1facbbc0a14ae6e1d4)

|  |
| --- |
| Describes how to add a member to an existing user role. |

[How to Create a User Role](#zb16f13fc2d5a4608a3676460515cbabf)

|  |
| --- |
| Describes how to create a user role. |

Reference

[Appendix A - List of User Role Profiles in Service Manager](#z6cd6943652ab4d7aa3a30d33187b7d88)

About User Roles

At your company, 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 (CI) but not delete them, whereas others are allowed to create, update, and delete CIs.

In 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 usually corresponds to employees’ 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 company may decide to separate the group of employees who maintain CIs in two groups: those who handle CIs for desktop computers and those who handle CIs for portable computers. They want to retain these two user role profiles, one that can create and edit, but not delete CIs, and another that can create, edit, and delete CIs. 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 that 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. Since the scope is undefined for these user roles; they can exercise their user profiles on all management pack, 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 |
| Service Manager Activity Implementers | Activity Implementers | Global |
| Service Manager Administrators | Administrators | Global |
| Service Manager Advanced Operators | Advanced Operators | Global |
| Service Manager Change Initiators | Change Initiators | Global |
| Service Manager End Users | End Users | Global |
| Service Manager Read-Only Operators | Read-Only Operators | Global |
| Service Manager Authors | Authors | Global |
| Service Manager Problem Analysts | Problem Analysts | Global |
| Service Manager Workflows | Workflows | Global |
| Service Manager Incident Resolvers | Incident Resolvers | Global |
| System Center Change Managers | Change Managers | Global |
| Service Manager Report Users\* | Report Users | Global |
| Release Manager |  |  |
| Activity Designer |  |  |

Note

The Service Manager Report Users user role is only available 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, you want to define one security access that allows users to create and edit, but not delete CIs, and another security access that allows users to create, edit, and delete CIs. 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 Users | No | No | No |
| Read-Only Operators | No | No | No |
| Activity Implementers | No | No | No |
| Change Initiators | No | No | No |
| Incident Resolvers | No | No | No |
| Problem Analysts | No | No | No |
| Change Manager | No | No | No |
| Advanced Operators | Yes | Yes | No |
| Authors | Yes | Yes | Yes |
| Workflows | Yes | Yes | No |
| Administrators | Yes | Yes | Yes |

Using the table above, you can see that the Advanced Operators user role profile can create and update, but not delete CIs. The Authors user role profile can create, update, and delete CIs. These are the two user role profiles you use to set up asset management at your company. The members of the asset management team who are allowed to create and update, but not delete CIs, 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 CIs are made members of the predefined Authors profile.

As a best practice, assume members of the asset management team might change. You create two groups in Active Directory and make those groups a member of the Advanced Operators and Authors profiles. Then as members change, users are added and removed from the group in Active Directory 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, create your own user role by using the same user role profiles, but with different scopes.

Why Some User Roles Cannot Be Created

When creating a user role, notice that four user roles are not listed: Administrator, End Users, Report User, and Workflows. These four 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.

End Users

By default, the End Users user role contains a list of all authenticated users, and similar to the Administrator user role, there is no reason for creating additional user roles like this.

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 the 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.

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 it is this user role that will perform the required actions on the Service Manager database. Like the Report User user role, the narrow purpose of this user role means there is no reason for creating other user roles.

See Also

[How to Add a Member to a User Role](#z3df2547120944e1facbbc0a14ae6e1d4)

[How to Create a User Role](#zb16f13fc2d5a4608a3676460515cbabf)

How to Add a Member to a User Role

Use the following procedure to assign users to a user role. In this example, you have to add members of an asset management team who can create and update, but not delete, configuration items. Looking at the “Configuration Items” section of Appendix A, you see that the Advanced Operators user role profile provides what you need. At this time, all members of the asset management team are responsible for every asset in the company, so that they require unlimited scope. Use the following procedure to add a user to the Service Manager Advanced Operators 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 to access rights, as specified in the user role. |

How to Create a User Role

Use the following procedure to create a user role and assign users to that 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 following these guidelines:  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 assigned access to, such as Incident Management Library. In addition, select the Service Manager Authoring Management Pack management pack, and click Next.  d. On the Classes page, select the classes that this user role will have access to, and click Next.  e. On the following pages, all the queues, groups, tasks, views, and form templates 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, then on the Groups page, Select all Groups is automatically selected. In addition, by default, no groups have been created. You have to create a group if you want to limit scope by group.  f. 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 for this user role, and click Next.  g. On the Summary page, make sure that the settings are correct, and click Create.  h. On the Completion page, make sure that The user role was created successfully appears, and 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. |

Managing Run As Accounts

During the setup of Service Manager, you specified credentials for the workflow and service accounts. If, because of the configurations of password security requirements used at your company, 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, an 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".

In This Section

[How to Change the User Credentials for the Operational System Run As Account](#za3bff9f556bf4ce19eb151742582ed51)

|  |
| --- |
| 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 System Run As Account](#z1f432350783d4242aaf2a39c39a71c40)

|  |
| --- |
| 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](#zc17ddd8e22de4b4abf94399490a6c578)

|  |
| --- |
| Describes how to update the workflow account if either the user name or password has changed. |

How to Change the User Credentials for the Operational System Run As Account

If the user account for the Operational System Run As account changes, you must make changes in the following locations:

1. The local administrators account on the Service Manager computers

2. The Service Manager Administrators user role for both the Service Manager and data warehouse management servers

3. The logon account for the System Center Data Access Service and System Center Management Configuration services

Note

The logon account for the System Center Management service is always the local system account and must not be changed.

4. The SQL Server logon account on computers hosting Service Manager databases

5. The Self-Service Portal application pool account

6. The Operational Run As 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 – 6. |

To change the logon account for the System Center Data Access Service and System Center 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, follow 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 System Run As 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 System Center 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, follow 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 System Run As 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 System Center 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, follow 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, follow 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 System Run As 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 System Run As account. In the Password and Confirm password boxes, type the password for the new Operational System Run As 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 System Run As 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 System Account.  4. In the Tasks pane, click Properties.  5. In the Operational System Account page, in the User name, Password, and Domain boxes, type the new credentials for the Operational System Run As account, and then click OK. |

How to Change the Password for the Operational System Run As Account

To change the log-on password for the System Center Data Access and System Center 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 System Center 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 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.  Note  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. |

Managing Knowledge Articles in Service Manager

Knowledge articles 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.

In This Section

[How to Create a Knowledge Article](#z9f906d2928cd4560bd3c4835c42a7a67)

|  |
| --- |
| Describes how to create a knowledge article. |

[How to Search for a Knowledge Article](#ze6060a9d350f40bf90e7eca0dc464dee)

|  |
| --- |
| Describes how to search for a knowledge article. |

How to Create a Knowledge Article

You can use the following procedure to create a knowledge article in System Center Service Manager 2010. This procedure describes how to create a new knowledge article to help users obtain the latest service pack for Windows Vista. However, you can follow 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 follow these steps:  a. In the Keywords box, type classification keywords that you can later search, separated by semi-colons. 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 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 Service Manager 2010. 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 0x123 error 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, so 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 0x123 error.  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 0x123 error. |

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 0x123 error.  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. |

Using the Service Manager Cmdlets for Windows PowerShell

This section provides an introduction to the System Center Service Manager cmdlets for Windows PowerShell.

In This Section

[Getting Started with Service Manager Cmdlets for Windows PowerShell](#zca96a2e1db474af2968c40f627336675)

|  |
| --- |
| Describes how to add the Service Manager snap-in to a Windows PowerShell session and how to get help for the cmdlets. |

[List of the Service Manager Cmdlets](#z417c5d92cf19494985f430b3b5b13399)

|  |
| --- |
| Provides a list of the cmdlets in the Service Manager snap-in for Windows PowerShell. |

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. Service Manager includes several 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 set includes cmdlets that operate on the data warehouse database, and, therefore, you typically run them on the data warehouse management server. The rest of the Service Manager cmdlets are typically run on the Service Manager management server

Data returned from Windows PowerShell command might contain more information than can be displayed in a default Windows PowerShell command window. We recommend increasing the width to 120. Right-click the title bar, click Properties, and in the Layout tab, set the Screen Buffer Size width to 120.

Every time you start a Windows PowerShell session to run a Service Manager cmdlet, you must first add the Service Manager Windows PowerShell snap-in as described below.

To add the Service Manager Windows PowerShell snap-in to a Windows PowerShell session

|  |
| --- |
| 1. On the computer that you run Windows PowerShell on, for example, the computer that hosts the Service Manager or data warehouse management server, on the taskbar, click Start, point to Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. In the Windows PowerShell window, type the following commands:  Set-ExecutionPolicy RemoteSigned  Add-PSSnapIn SMCmdletSnapIn |

To verify that the Service Manager Windows PowerShell snap-in has been added

|  |
| --- |
| 1. On the taskbar, click Start, point to Programs, point to Windows PowerShell 1.0, and then click Windows PowerShell to open a Windows PowerShell window.  2. Type the following command, and look for Service Manager cmdlets such as Add-SCDWMgmtGroup and Export-SCSMManagementPack:  Add-PSSnapIn SMCmdletSnapIn  Get-Command –pssnapin SMCmdletSnapIn  Tip  Tab completion is a simple method that you can use to verify that a Windows PowerShell cmdlet has been added. For example, you can type Add-SC, and then press the Tab key, which automatically completes the command. |

To get Help for a cmdlet

|  |
| --- |
| 1. On the taskbar, click Start, point to Programs, point to Windows PowerShell 1.0, and then click Windows PowerShell to open a Windows PowerShell window.  2. Type the following command. Replace <cmdlet-name> with the name of the cmdlet that you must get help for, for example, Import-SCSMManagementPack:  Add-PSSnapIn SMCmdletSnapIn  get-help <cmdlet-name> -detailed |

List of the Service Manager Cmdlets

System Center Service Manager 2010 supports the following cmdlets.

Service Manager Cmdlets

|  |  |
| --- | --- |
| Cmdlet | Description |
| Get-SCSMManagementPack | Gets the Service Manager management packs that have been imported into a specific system. |
| Import-SCSMManagementPack | Imports a management pack into Service Manager. |
| Export-SCSMManagementPack | Exports a management pack as a valid XML-formatted file that you can later import into Service Manager. |
| Get-SCSMConnector | Gets the connectors that are currently installed on the system, displaying for each returned connector the type, name, and status information. |
| Set-SCSMConnector | Enables or disables connectors. |
| Get-SCSMRunAsAccount | Gets the Run As accounts available in the Service Manager environment. |
| Set-SCSMRunAsAccount | Sets the credentials for a Run As account. |
| Import-SCSMInstance | Imports objects and relationships into Service Manager. |
| Add-SCDWMgmtGroup | Registers a Service Manager management group and its servers as a source for the data warehouse. |
| Disable-SCDWJob | Disables a data warehouse job to prevent it from running. |
| Disable-SCDWJobSchedule | Disables a data warehouse job schedule, which causes the job schedule to stop starting jobs. |
| Enable-SCDWJob | Enables a data warehouse job so that it can run according to its schedule. |
| Enable-SCDWJobSchedule | Allows data warehouse administrators to enable job schedules so that jobs run according to their specified schedule. |
| Get-SCDWJob | Gets the job information and status of all recurring jobs, including extract, transform, and load jobs. |
| Get-SCDWJobModule | Gets detailed information for the specified job. This information includes job modules that are executed as part of the job. |
| Get-SCDWJobSchedule | Displays scheduling information for data warehouse jobs. |
| Get-SCDWMgmtGroup | Displays details about the management groups that are registered with the data warehouse. |
| Remove-SCDWMgmtGroup | Unregisters a Service Manager management group and its associated servers as a data warehouse data source. |
| Resume-SCDWJob | Resumes a suspended job. |
| Set-SCDWJobSchedule | Sets the schedule for a data warehouse job. |
| Start-SCDWJob | Starts a data warehouse job. |
| Suspend-SCDWJob | Suspends operation of the specified job after all of its running job modules are complete. Any job modules that are queued to begin as part of the job will not run until the job is resumed. |

Managing the Data Warehouse in Service Manager

This section provides an overview of the key concepts that you have to understand to manage the data warehouse in System Center Service Manager 2010. This section also contains procedures that you can use to manage the data warehouse.

In This Section

[About Managing the Data Warehouse](#z6719523c7262496ebe3b48080c18e949)

|  |
| --- |
| Provides an overview of key concepts that you have to understand to manage the data warehouse. |

[How to Disable a Data Warehouse Job Schedule](#zfe31c9b2f5d14ef7b3a2f0cb8a837c61)

|  |
| --- |
| Describes how to disable data warehouse job schedules. |

[How to Enable Data Warehouse Job Schedules](#zd9206d95ad4d4606a0ed63f90dc26bb1)

|  |
| --- |
| Describes how to enable data warehouse job schedules. |

[How to View the Status of a Data Warehouse Job](#z9151b4974dfd4ffb9d504b41a8a31a6a)

|  |
| --- |
| Describes how to view the job status in the data warehouse. |

[How to Suspend and Resume a Data Warehouse Job](#ze008ab1279d446d891fdebdccb26bfa8)

|  |
| --- |
| Describes how to pause and resume data warehouse jobs. |

[How to Schedule a Data Warehouse Job](#zb3dff8c0b490451f9f5bff49c02ae6ea)

|  |
| --- |
| Describes how to schedule data warehouse jobs. |

[How to View Data Warehouse Job History](#za9dff36cf6f547aa97585a7f63027e61)

|  |
| --- |
| Describes how to view the data warehouse job history. |

[How to Troubleshoot a Data Warehouse Job](#z392112d6e35747a7aadbfbe5ab4677e7)

|  |
| --- |
| Describes how to troubleshoot data warehouse jobs. |

About Managing the Data Warehouse

In Service Manager, there are seven data warehouse jobs that run at various times in order 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 takes several hours to complete on its initial run. For more information, see ”Register with Service Manager Data Warehouse” in the [System Center Service Manager Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=129134) (http://go.microsoft.com/fwlink/?LinkId=129134). |
| DWMaintenance | This job performs data warehouse maintenance, such as indexing and updating statistics. This job will automatically run after the MPSyncJob has finished. |
| Entity (or Grooming) | Grooming functions typically involve activities 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 used for all end user reporting needs. |

For more information about the extract, transform, and load (ETL) jobs, see the blog posting [Data Warehouse – Anatomy of Extract, Transform, Load (ETL)](http://go.microsoft.com/fwlink/?LinkId=164088) (http://go.microsoft.com/fwlink/?LinkId=164088).

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. All of these maintenance tasks can be performed by using PowerShell commands. In addition, some of these tasks can be performed through the Service Manager console. The following procedures provide instructions for using PowerShell and using the Service Manager console as appropriate.

During deployment, you registered the Service Manager management group as discussed in “Register Service Manager Management Group” in the [System Center Service Manager Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=129134) (http://go.microsoft.com/fwlink/?LinkId=129134). As a result of that action, management pack deployment started and MPSyncJob started. You should not start or resume any data warehouse jobs until the MPSyncJob has finished, as shown in the Data Warehouse Jobs pane in the Service Manager console.

In the following procedures, you can manage the data warehouse by using a combination of Windows PowerShell cmdlets and the Service Manager console to perform tasks with data warehouse jobs.

|  |  |
| --- | --- |
| Task | Reference |
| Enable data warehouse jobs | [How to Enable Data Warehouse Job Schedules](#zd9206d95ad4d4606a0ed63f90dc26bb1) |
| View data warehouse jobs status | [How to View the Status of a Data Warehouse Job](#z9151b4974dfd4ffb9d504b41a8a31a6a) |
| Start and stop data warehouse jobs when you have to | [How to Suspend and Resume a Data Warehouse Job](#ze008ab1279d446d891fdebdccb26bfa8) |
| Schedule data warehouse jobs on a recurring basis | [How to Schedule a Data Warehouse Job](#zb3dff8c0b490451f9f5bff49c02ae6ea) |
| Determine whether data warehouse jobs are running as expected | [How to Troubleshoot a Data Warehouse Job](#z392112d6e35747a7aadbfbe5ab4677e7) |

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 snap-in for Windows PowerShell 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—Gets current 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.

When you run Windows PowerShell cmdlets for the first time, you must set the execution policy to RemoteSigned. Then, each time you run a Windows PowerShell cmdlet, you must run the Add-PSSnapin command to add the Service Manager snap-in. For more information about these commands, see [Getting Started with Service Manager Cmdlets for Windows PowerShell](#zca96a2e1db474af2968c40f627336675).

Getting Started with Data Warehouse Jobs

When you register with the Service Manager data warehouse (see "Register with Service Manager Data Warehouse" in the [System Center Service Manager Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=129134) http://go.microsoft.com/fwlink/?LinkId=129134), 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 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.

How to Disable a Data Warehouse Job Schedule

Use the following procedure to disable the schedule for the ETL jobs; however, this procedure can be used to disable the schedule for any data warehouse job. In this release of Service Manager, you can disable the schedules only by using Windows PowerShell. Additionally, in this release, it is not possible to query for the status of a data warehouse job schedule.

Note

To run the commands in this topic, the execution policy in Windows PowerShell must be set to RemoteSigned. For more information about how to set the execution policy, see [Getting Started with Service Manager Cmdlets for Windows PowerShell](#zca96a2e1db474af2968c40f627336675).

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 Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER:  Add-PSSnapIn SMCmdletSnapIn  3. Type the following commands, and then 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  4. Type exit, and then press ENTER. |

How to Enable Data Warehouse Job Schedules

By default, the schedules for the extract, transform, and load (ETL) jobs are not enabled. Use the following procedure to enable the schedule for the ETL jobs; however, this procedure can be used to enable the schedule for any of the data warehouse jobs. In this release of Service Manager, you can enable the schedules only by using Windows PowerShell. Additionally, in this release, it is not possible to query for the status of a data warehouse job schedule. If you have to know the status of a particular job, run the command to enable it.

Note

To run the commands in this topic, the execution policy in Windows PowerShell must be set to RemoteSigned. Type the command Set-ExecutionPolicy RemoteSigned to set the execution policy.

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 Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell command prompt, type the following command, and then press ENTER:  Add-PSSnapIn SMCmdletSnapIn  3. 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  4. Type exit, and then press ENTER. |

How to View the Status of a Data Warehouse Job

You can use the following procedures to view the data warehouse job status to determine whether a job is running, stopped, or failed.

Note

To run the Windows PowerShell cmdlets, the execution policy in Windows PowerShell must be set to RemoteSigned. For more information, see [Getting Started with the Service Manager Cmdlets](http://go.microsoft.com/fwlink/?LinkId=178233) (http://go.microsoft.com/fwlink/?LinkId=178233) in the System Center Service Manager Administrator’s Guide.

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 Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. Type the following command, and then press ENTER.  Get-SCDWJob  4. Review the list of jobs to view their status. |

How to Suspend and Resume a Data Warehouse Job

You can suspend (or pause) and resume data warehouse jobs that are running. For example, you might have to suspend 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 suspend (or pause) and then resume 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

To run the Windows PowerShell cmdlets, the execution policy in Windows PowerShell must be set to RemoteSigned. For more information, see [Getting Started with the Service Manager Cmdlets](http://go.microsoft.com/fwlink/?LinkId=178233) (http://go.microsoft.com/fwlink/?LinkId=178233) in the System Center Service Manager 2010 Administrator’s Guide.

To pause and resume 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 suspended in the Data Warehouse Jobs pane, and then click Resume in the Tasks list. |

To suspend all data warehouse jobs using Windows PowerShell cmdlets

|  |
| --- |
| 1. On the computer that hosts the data warehouse management server, click Start, point to Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. Type the following commands, and then press ENTER after each command.  Suspend-SCDWJob –JobName Extract\_<data warehouse management group name>  Suspend-SCDWJob –JobName Extract\_<Service Manager management group name>  Suspend-SCDWJob –JobName Transform.Common  Suspend-SCDWJob –JobName Load.Common  4. Type exit, and then press ENTER. |

To resume all data warehouse jobs using Windows PowerShell cmdlets

|  |
| --- |
| 1. On the computer that hosts the data warehouse management server, click Start, point to Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. Type the following commands, and then press ENTER after each command.  Resume-SCDWJob –JobName Extract\_<data warehouse management group name>  Resume-SCDWJob –JobName Extract\_<Service Manager management group name>  Resume-SCDWJob –JobName Transform.Common  Resume-SCDWJob –JobName Load.Common  4. Type exit, and then press ENTER. |

How to Schedule a Data Warehouse Job

You can use the following procedure to schedule a data warehouse job in System Center Service Manager 2010.

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](http://go.microsoft.com/fwlink/?LinkId=129134) (http://go.microsoft.com/fwlink/?LinkId=129134) in the System Center Service Manager Deployment Guide.

In the following procedure, you set 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 schedule data warehouse jobs

|  |
| --- |
| 1. On the computer that hosts the data warehouse management server, click Start, point to Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. 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 Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. Type the following command, and then press ENTER:  Get-SCDWJobSchedule |

How to View Data Warehouse Job History

A history of data warehouse jobs is collected as they run. 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 Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. Type the following command, and then press ENTER.  Get-SCDWJob -NumberOfBatches 5  4. Type exit, and then press ENTER. |

How to Troubleshoot a Data Warehouse Job

In System Center Service Manager 2010, 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, point to Programs, point to Windows PowerShell 1.0, right-click Windows PowerShell, and then click Run as administrator.  2. At the Windows PowerShell command prompt, type the following command, and then press ENTER.  Add-PSSnapIn SMCmdletSnapIn  3. Type the following command, and then press ENTER.  Get-SCDWJob  4. Review the output, and locate any job with a status of "Failed."  5. 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  6. 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.  7. When you are ready to retry the failed job, type the following command, and then press ENTER.  Resume-SCDWJob -JobName Transform.Common |

Managing the Self-Service Portal

The Self-Service Portal is used by end users to contact help desk personnel for help requests. Users can also view announcements, search the knowledge base, perform tasks, and manage their requests. In particular, an important task they can perform includes requesting software, which is deployed as a software package by System Center Configuration Manager. Items in the Portal node of the Service Manager console are used to inform users about help desk personnel contact information and to configure software approval and deployment processes. Items in the Portal node are also used to specify information about Configuration Manager so that Service Manager can retrieve software packages. Use the following procedures to configure the Self-Service Portal so that users can request software.

Note

When you view a software package in the Self-Service Portal, software packages that are classified under multiple deployment processes appear only in the last deployment process or category in which the package was classified.

In This Section

[How to Set the Configuration Manager Configuration](#zbe9bcf0cb3ca4c028142041cc30aaa0d)

|  |
| --- |
| Describes how to set the Configuration Manager configuration that is used by Service Manager to retrieve software packages. |

[How to Set End User Portal Contact IT Settings](#z86ab6bc2f66f4f4f81f5accae60078c5)

|  |
| --- |
| Describes how to publish contact information that Self-Service Portal users can view. |

[How to Configure a Software Deployment Process](#z77a793c8cc5642b29c16b5347cac45f1)

|  |
| --- |
| Describes how you can configure software deployment processes for approval and deployment. |

[How to Publish Software Packages](#z37fb2cb88792461b9e832791ab7b44b5)

|  |
| --- |
| Describes how you can publish software packages in the Service Manager console. |

How to Set the Configuration Manager Configuration

Use the following procedure to provide information about the System Center Configuration Manager central site server; System Center Service Manager 2010 uses this information for self-service software provisioning. The site server information you specify is used by Service Manager to connect to the site server. Later, using the software deployment process you create, the site server information is also used to import the software package list. The software package list is made available to Self-Service Portal users so that they can request software.

To set the Configuration Manager central site settings

|  |
| --- |
| 1. In the Service Manager console, click Administration.  2. In the Administration pane, expand Portal, and then click Settings.  3. In the Settings pane, click Configuration Manager Software Deployment Configuration.  4. In the Tasks pane, under Configuration Manager Software Deployment Configuration, click Properties.  5. In the Configuration Manager Configuration dialog box, in the Site server name box, type the name of the Configuration Manager 2007 central site server.  6. In the Site code box, type the three-character site code.  7. Optionally, in the Description box, type a description of the central site server.  8. Click OK to save and close. |

See Also

[How to Configure a Software Deployment Process](#z77a793c8cc5642b29c16b5347cac45f1)

How to Set End User Portal Contact IT Settings

In System Center Service Manager 2010, use the following procedure to provide information to Self-Service Portal users so that they can contact your IT help desk. After you follow the steps in the procedure, Self-Service Portal users can click Contact IT to display the Contact support box.

All information that you enter is optional. For example, if your organization does not use instant messaging, you can leave the corresponding field empty.

To set the end user portal contact IT settings

|  |
| --- |
| 1. In the Service Manager console, click Administration.  2. In the Administration pane, expand Portal, and then click Settings.  3. In the Settings pane, click End-user portal contact IT settings.  4. In the Tasks pane, under End-user portal contact IT settings, click Properties.  5. In the Self-service portal contact settings dialog box, in the E-mail address box, type the e-mail address that your help desk uses to receive incident requests.  6. In the E-mail response time box, type the approximate time that your organization takes to reply to user e-mail messages. You can also specify the working hours and the days of the week when the help desk is available.  7. In the Support phone box, type the phone number that your help desk uses to receive phone calls.  8. In the Fax number box, type the fax number that your help desk uses to receive faxes.  9. In the Chat URL name box, type the name that you want to display to users so that they can start an instant message conversation with a help desk technician.  10. In the Chat URL field, type the URL that your instant messaging infrastructure is configured to use to receive incoming instant message requests. For example, type sip:helpdesk@woodgrove.com.  11. In the Chat response time field, type the approximate time that your organization takes to reply to user chat requests. You can also specify the working hours and the days of the week when the help desk is available.  12. Click OK to save and close. |

How to Configure a Software Deployment Process

In System Center Service Manager 2010, use the following procedure to define a process that your organization can use to approve a software deployment request that an end user initiates from the Self-Service Portal. Software packages are imported from Configuration Manager using other procedures; the process you create by using the following procedure allows the software deployment request to be approved.

End users submit change requests in the Self-Service Portal if they want to install software. After all the approval processes are completed successfully, the requested software is installed by Configuration Manager on the end user’s computer. You can define multiple software deployment processes for your organization to manage various software titles and suites and to apply different approval and implementation processes based on change request templates.

If you create a change request template for a custom review activity that requires line manager approval and the template is later linked to a software deployment process, the software request is automatically, although incorrectly, approved. This error only occurs when a Self-Service Portal user who is not a Service Manager user requests the software. Therefore, as a best practice, when you create a change request template, you must add specific reviewers. For more information about adding a change reviewer, see How to Add a Change Reviewer in the System Center Service Manager Operations Guide. This incorrect approval condition has been corrected in Service Manager 2010 Service Pack 1.

Note

Although you can base a software deployment process on your own custom change request template, Service Manager does not correctly display the change request template name in the Software Deployment Process list. However, the software deployment process still functions correctly.

To create a software deployment process

|  |
| --- |
| 1. In the Service Manager console, click Administration.  2. In the Administration pane, expand Portal, and then click Software Deployment Process.  3. In the Software Deployment Process pane, click Create.  4. In the General section in the Name box, type the name of the process you want to create. For example, type Standard Microsoft Office Software Request Process.  5. In the Description box, type a description of the process. For example, type Use this process to approve and deploy Microsoft Office software to end users.  6. In the Process section under Create a software deployment process, click Select to open the Select objects list, and then view the list of available software packages.  7. In the list, select a software package, click Add, and then click OK.  8. Under Templates, select a template to apply to the software deployment process, and then click OK to save and close the form.  9. Click OK to save and close the form. |

How to Publish Software Packages

In System Center Service Manager 2010, use the following procedure to publish software packages that are displayed to end users in the Self-Service Portal. End users see this list of software packages when they request software. You can publish or unpublish software packages using the Software Packages view in the Service Manager console.

To publish software packages

|  |
| --- |
| 1. In the Service Manager console, click Administration.  2. In the Administration pane, expand Portal, and then click Software Packages.  3. In the Software Packages view, select one or more items to publish. Then, in the Tasks list, click Publish.  4. The items you selected for publishing are listed as True in the Publish column.  5. If you receive an error when you try to publish a package, you might need to configure the package. To configure the package, follow these steps:  a. Select a software package.  b. In the Tasks list, click Configure.  c. Select the program that should run, ensure that Publish this package to the self-service portal is selected, and then click OK. |

See Also

[How to Configure a Software Deployment Process](#z77a793c8cc5642b29c16b5347cac45f1)

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 the Event Viewer. The Event Viewer reads logs from remote computers.

In System Center Service Manager 2010, 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 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 computers related to the incident.

In This Section

[How to Create a Task](#z69dd3c46b3f44eda85317c3cdc047906)

|  |
| --- |
| Describes how to create a task. |

[How to Run a Task From an Incident View](#za81905ce717d4e76bcd28cafadb015df)

|  |
| --- |
| Describes how to run a task from an incident view. |

How to Create a Task

Use the following procedure to create a task; for example, a task that you can use to open Event Viewer and view logs on a computer. The 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, perform 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 the Event Viewer starts, and the events from the computer associated with the incident are displayed. |

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.

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 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. |

To Configure Service Manager CEIP Settings

During setup, on the Help improve System Center page, you have the option to participate in the Customer Experience Improvement Program (CEIP). You can use the following procedure to either let Service Manager participate in the program or remove Service Manager from this program.

To configure Service Manager CEIP settings

|  |
| --- |
| 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 perform 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. |

Appendix A - List of User Role Profiles in Service Manager

This appendix provides information about the user role profiles in Service Manager.

Knowledge

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User Role Profile | Read Knowledge Articles | Create Knowledge Articles | Edit Knowledge Articles | Delete Knowledge Articles |
| Report User | No | No | No | No |
| End Users | Yes | No | No | No |
| Read-Only Operators | Yes | No | No | No |
| Activity Implementers | Yes | No | No | No |
| Change Initiators | Yes | No | No | No |
| Incident Resolvers | Yes | No | No | No |
| Problem Analyst | Yes | No | No | No |
| Change Managers | Yes | No | No | No |
| Advanced Operators | Yes | Yes | Yes (CI Group Scope) | No |
| Authors | Yes | Yes | Yes (CI Group Scope) | Yes |
| Workflows | Yes | Yes | Yes | No |
| Administrators | Yes | Yes | Yes | Yes |

Work Items

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| User Role Profile | Create Work Items from All Work Item Classes | Create Change Requests and Activities | Edit Work Items from All Work Item Classes | Edit Activities and Change Requests | Edit Manual Activities (Status and Comment Fields) | Edit Incidents, Problems, Manually Activities | Delete Work Items |
| Report User | No | No | No | No | No | No | No |
| End Users | Yes | Yes | No | No | No | No | No |
| Read -Only Operators | No | No | No | No | No | No | No |
| Activity Implementers | No | No | No | No | Yes (WI Queue Scope) | No | No |
| Change Initiators | No | Yes | No | No | No | No | No |
| Incident Resolvers | No | No | No | No | Yes (WI Queue Scope) | Yes (WI Queue Scope) | No |
| Problem Analyst | No | No | No | No | Yes (WI Queue Scope) | Yes (WI Queue Scope) | No |
| Change Managers | No | Yes | No | Yes (WI Queue Scope) | Yes (WI Queue Scope) | No | No |
| Advanced Operators | Yes | Yes | Yes (WI Queue Scope) | Yes (WI Queue Scope) | Yes (WI Queue Scope) | Yes (WI Queue Scope) | No |
| Authors | Yes | Yes | Yes (WI Queue Scope) | Yes (WI Queue Scope) | Yes (WI Queue Scope) | Yes (WI Queue Scope) | No |
| Workflows | Yes | Yes | Yes | Yes | Yes | Yes | No |
| Administrators | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

Configuration Items

|  |  |  |  |
| --- | --- | --- | --- |
| User Role Profile | Create Configuration Items | Update Configuration Items | Delete Configuration Items |
| Report User | No | No | No |
| End Users | No | No | No |
| Read-Only Operators | No | No | No |
| Activity Implementers | No | No | No |
| Change Initiators | No | No | No |
| Incident Resolvers | No | No | No |
| Problem Analyst | No | No | No |
| Change Managers | No | No | No |
| Advanced Operators | Yes | Yes (CI Group Scope) | No |
| Authors | Yes | Yes (CI Group Scope) | No |
| Workflows | Yes | Yes | No |
| Administrators | Yes | Yes | Yes |

Implied Permissions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Role Profile | Read and Edit Reviewer (Vote and Comment Properties Only) Where The User Is The Reviewer | Read and Edit Incidents Where The User Is The Affected User | Read but Not Edit CIs Where The User Is The Affected User | Work Items Assigned to User | Read but Not Edit Computers Where The User Is The Primary User |
| Report User | No | No | No | No | No |
| End Users | Yes | Yes | Yes | Yes | Yes |
| Read-Only Operators | Yes | Yes | Yes | Yes | Yes |
| Activity Implementers | Yes | Yes | Yes | Yes | Yes |
| Change Initiators | Yes | Yes | Yes | Yes | Yes |
| Incident Resolvers | Yes | Yes | Yes | Yes | Yes |
| Problem Analyst | Yes | Yes | Yes | Yes | Yes |
| Change Managers | Yes | Yes | Yes | Yes | Yes |
| Advanced Operators | Yes | Yes | Yes | Yes | Yes |
| Authors | Yes | Yes | Yes | Yes | Yes |
| Workflows | Yes | Yes | Yes | Yes | Yes |
| Administrators | Yes | Yes | Yes | Yes | Yes |

Notifications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User Role Profile | Create Personal Notification Subscriptions | Create Global Notification Subscriptions | Edit Notification Channels | Create and Edit Notification Templates |
| Report User | Yes | No | No | No |
| End Users | No | No | No | No |
| Read-Only Operators | Yes | No | No | No |
| Activity Implementers | Yes | No | No | No |
| Change Initiators | Yes | No | No | No |
| Incident Resolvers | Yes | No | No | No |
| Problem Analyst | Yes | No | No | No |
| Change Managers | Yes | No | No | No |
| Advanced Operators | Yes | No | No | No |
| Authors | Yes | No | No | No |
| Workflows | No | No | No | No |
| Administrators | Yes | Yes | Yes | Yes |

Authoring

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| User Role Profile | Create and Edit Views | Create and Edit Tasks | Create and Edit Templates | Create and Edit Groups | Create and Edit Queues | Create, Edit, and Delete List Items |
| Report User | No | No | No | No | No | No |
| End Users | No | No | No | No | No | No |
| Read-Only Operators | No | No | No | No | No | No |
| Activity Implementers | No | No | No | No | No | No |
| Change Initiators | No | No | No | No | No | No |
| Incident Resolvers | No | No | No | No | No | No |
| Problem Analyst | No | No | No | No | No | No |
| Change Managers | No | No | No | No | No | No |
| Advanced Operators | No | No | No | No | No | No |
| Authors | Yes (Class Scoped) | Yes (Class Scoped) | Yes | No | No | Yes |
| Workflows | No | No | No | No | No | No |
| Administrators | Yes | Yes | Yes | Yes | Yes | Yes |

Administration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User Role Profile | Create, Edit, and Delete User Roles | Import, Export, and Delete Management Packs | Create, Edit, and Delete Connectors | Configure Workflows |
| Report User | No | No | No | No |
| End Users | No | No | No | No |
| Read-Only Operators | No | No | No | No |
| Activity Implementers | No | No | No | No |
| Change Initiators | No | No | No | No |
| Incident Resolvers | No | No | No | No |
| Problem Analyst | No | No | No | No |
| Change Managers | No | No | No | No |
| Advanced Operators | No | No | No | No |
| Authors | No | No | No | No |
| Workflows | No | No | No | No |
| Administrators | Yes | Yes | Yes | Yes |

Appendix B - Mapping Active Directory Domain Services Attributes to Service Manager Properties

Using an Active Directory connector, System Center Service Manager 2010 synchronizes data with the User, Group, Computer, and Printer Active Directory Domain Services objects. The tables below display the mapping between the attributes of the Active Directory Domain Services 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 |
| 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 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 |
| 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 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 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 display 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 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.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 |
|  | 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 |
|  | 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 |
|  | 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 |
|  | Language | SCCM\_Ext.vex\_Package.Language |
|  | Manufacturer | SCCM\_Ext.vex\_Package.Manufacturer |
|  | Description | SCCM\_Ext.vex\_Package.Description |

Appendix D - 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 Service Manager 2010 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 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 the 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 Manager\Console\ConsoleDisplaySettings\TasksPaneExpanded | The Tasks 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\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. |
| 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 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 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 the section are used to manage functions internal to Service Manager.

|  |  |
| --- | --- |
| Key | Description and values |
| HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\System Center\2010\Common\GroupCalcPollingIntervalMilliseconds | Specifies the group change check interval in milliseconds. For more specific information, see the [System Center Service Manager 2010 SP1 Planning Guide](http://go.microsoft.com/fwlink/?LinkId=207215) (http://go.microsoft.com/fwlink/?LinkId=207215). |