Installing Cisco Physical Security Operations Manager Release 6.1

Revised February 11, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28434-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Installing Cisco Physical Security Operations Manager Release 6.1

CONTENTS

CHAPTER 1

PSOM Architecture Overview

This chapter provides an overview of the Cisco Physical Security Operations Manager (PSOM) architecture.

This chapter includes these topics:

Understanding the Deployment Architecture

PSOM includes these major components:

- PSOM Services—Collect information from various sensors within a security environment, and process this data for analysis of alert conditions. Specifically, the PSOM Services integrate with video, access control, and intrusion detection systems to collect sensor alerts and live and recorded video. Multiple network interface cards (NICs) enable PSOM Services to access the IP networks for the subsystems which may be on different networks.
- PSOM consoles—Includes the Administration Console, Operation Console, Alert Management Console, Video Management Console, and Business Logic Designer. The Operation Console enables operators to detect and respond to alerts, view live and recorded video, and report on alert conditions. The Administration Console enables administrators to configure and manage the elements of PSOM used by the Operation Console. See *Administering Cisco Physical Security Operations Manager* for details about all of the Consoles.
- PSOM Repository—Stores all environment configurations and data collected by PSOM in a standard Microsoft SQL Server 2008 database.

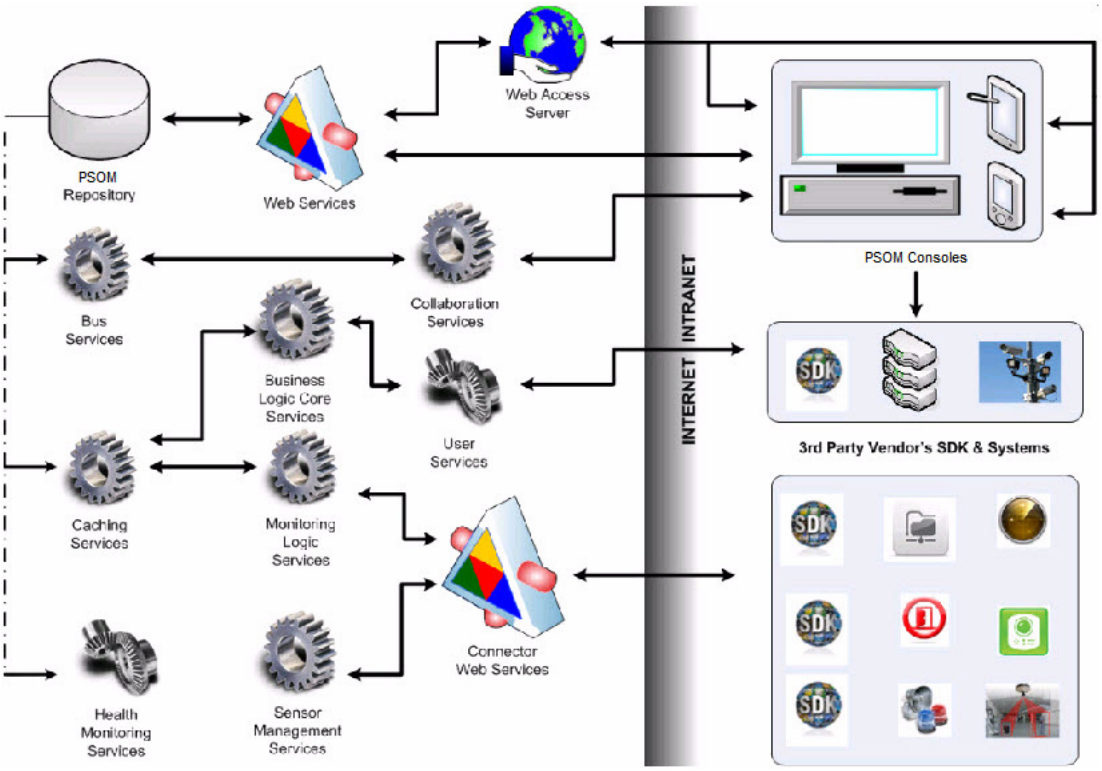
PSOM Services

Each of the PSOM services must be running for PSOM to function correctly.

- Bus Services (BUS)—Dispatches and routes rules, alerts, schedules, and commands to various services. Dynamically discovers Integration Modules and monitors services for abnormalities (for example, a service becomes unreachable).
- Caching Services (CS)—Speeds up business logic execution by caching monitoring hierarchy and sensor map information.

- Business Logic Core Services (BL CORE)—Runs business logic policies such as Alert Business Logic, Scheduled Business Logic, and so on. The BL CORE does not handle event monitoring logic.
- Monitoring Logic Services (MS)—Detects new and updated events from sensors via Integration Modules and creates alerts in PSOM.
- Sensor Management Services (SM)—Automatically discovers sensors via Integration Modules and synchronizes them with PSOM. Supports customized parsing of device semantics, and can automatically create the monitoring hierarchy with correct areas, zones and sensor locations.
- Web Services (WS)—Handles communication between PSOM Services and PSOM consoles, and enables integration with external alarm systems.
- User Services (US)—Runs reports on data collected by PSOM and controls video management systems and cameras. This service is optional.
- Connector Web Services (CWS)—Handles communication with third-party vendor systems via Integration Modules. This service is optional if only video is being used.
- Collaboration Services—Serves as the central service hub for end users to collaborate and communicate via instant messaging, as well as enables push notifications/subscriptions, and response workflow notifications.
- Health Monitoring Services—Monitors the PSOM system runtime behavior and health using agents that are polled to collect data and raise any alarms if necessary.
- Video Alert Services—Allows video adaptors to expose video alerts to Monitoring Services and Business Logic processing.

Note The PSOM Services can be self-contained on a single server or distributed across multiple servers.



PSOM uses a scalable Service Oriented Architecture (SOA) based on the Microsoft .NET Framework, and is composed of a series of web services, which means that PSOM enables easy integration with existing technology infrastructures.

Instead of being a monolithic application requiring significant development to add or modify functionality, PSOM uses a modern modular design that separates application components into discrete modules. The modular approach enables easy modifications with minimal impact and allows new functional modules to be added at any time. The PSOM integration modules with physical security subsystems leverage this approach for quick development and deployment.

All data collected by PSOM is stored in a standard Microsoft SQL Server 2008 database. The use of a commonly deployed database platform simplifies regular database administration tasks and allows easy access to data in case there are unique reporting requirements not met by the PSOM reporting capabilities. In addition to simplified management and reporting, PSOM can leverage some of the SQL Server more advanced features such as clustering and replication.

All communication between PSOM components is based on the global standard TCP/IP protocol. This communication uses standard port definitions such as HTTP or HTTPS, which means firewalls and other networking equipment require minimal configuration modifications. The message format used for communication is based on another industry standard, Extensible Markup Language, commonly known as XML. A significant benefit of using XML as a data interchange is that third party products based on SOA and XML can be quickly and easily integrated with PSOM.

Failover and Redundancy

The PSOM architecture supports a redundant multi-site and multi-hierarchy deployment whereby redundancy is achieved in several ways:

- PSOM Services redundancy—PSOM Services can be installed on multiple computers for redundancy and scalability.
- Server components redundancy—Microsoft Cluster Server or NEC ExpressCluster can be used for any and all PSOM components.
- Console redundancy—Multiple instances of PSOM Consoles can run simultaneously on machines spread out across the network.

Because PSOM architecture supports underlying communications systems (including failover capabilities of these systems), PSOM is redundant across control centers. If a failure occurs at one site, PSOM continues to operate using the redundant communications systems at the backup site.

When deploying PSOM to multiple security operations centers, each center should have its own PSOM Repository and PSOM Web Service configured to run on fault-tolerant Microsoft Windows Server 2008 R2 machines. Peer-to-peer replication in Microsoft SQL Server 2008 should be used to automatically replicate the databases between the security operations centers. Therefore, each center should have a local aggregate database and the replicated database for all sites. Failover is achieved via automated switching by the PSOM Web Service to the replicated database when the local database cannot be reached. In case of a catastrophic event, field operators can use VPN to connect to the backend components in any site.

CHAPTER 2

Preparing to Install PSOM

This chapter describes now to prepare your environment for a first-time installation of PSOM.

UCS Requirements

Cisco PSOM is installed on a a Cisco Unified Computing System (UCS) B-Series or C-Series server. Table 1 describes the requirements for these servers.

Table 1 UCS Requirements for PSOM

Subject	Requirements	Requirement Complete? (✓)
Platform Requirements	UCS B-Series Blades or UCS C-Series rack-mount server. See the data sheets for the latest guidelines: http://www.cisco.com/en/US/products/ps10818/products_data_sheets_list.html.	☐
	The platform must be configured with the required IP addresses for the management network.	☐
	Fiber Channel-based Storage Area Network (SAN) storage is installed for use by the UCS B-Series servers.	☐
vSphere Client Requirements	VMware Hypervisor version: ESXi 5.0	☐
	Cisco Unified Computing System Manager (UCSM) version: 1.4 and later	☐
VM Requirements	• Guest OS: Microsoft Windows 2008 R2 64-bit (Standard, Enterprise, or Datacenter) • CPU and memory recommendations for UCS B- and C-Series platforms: 4 vCPUs, 8 GB RAM, 500 GB hard disc • Microsoft SQL Server 2008 R2 64-bit (Standard or Enterprise Edition)	☐
PSOM Client Hardware Requirements	Same requirements as Cisco VSM client. See *Cisco Video Surveillance Monitoring Workstation Performance Baseline Specification, Release 7.0* for these requirements: http://www.cisco.com/en/US/products/ps10818/prod_technical_reference_list.html	☐

Summary of Deployment Steps

This section describes the general steps that you perform to deploy PSOM.

	Task	More Information	Task Complete? (✓)
Step 1	Install and configure the Cisco UCS platform.	• Cisco Unified Computing and Servers: http://www.cisco.com/en/US/products/ps10265/index.html • Cisco UCS Platform and VM documentation	☐
Step 2	Install and configure VMware.	• Installing and Configuring VMware Tools: http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf • VMware ESXi Configuration Guides: http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html • Cisco UCS Platform and VM documentation	☐
Step 3	Download the PSOM 6.1 software from Cisco.com to the UCS server.	Go to the following URL and choose **Products > Physical Security > Connected Physical Security**. http://software.cisco.com/download/navigator.html?mode=home	☐
Step 4	Create a virtual machine for PSOM 6.1 on the UCS server.	See the "UCS Requirements" section on page 2-1	☐
Step 5	Install Windows 2008 R2 64-bit.	• See the "UCS Requirements" section on page 2-1 • See Your Windows documentation	☐
Step 6	Verify that Microsoft .NET 4.0 SP1 is installed.	See the "Verifying that .NET Framework is Installed" section on page 2-8	☐
Step 7	Install SQL Server 2008 R2 32- or 64- bit.	See the "Installing SQL Server 2008 R2" section on page 2-8	☐
Step 8	Install necessary PSOM server software.	See the "Prerequisite Installation for PSOM Web Service and Connector Web Service" section on page 2-12	☐

	Task	More Information	Task Complete? (✓)
Step 9	Install Cisco Integration modules.	See these documents: • *Cisco Physical Access Manager Integration Module for Cisco Physical Security Operations Manager* • *Cisco IPICS Integration Module for Cisco Physical Security Operations Manager* • *Cisco VSM 6.3 Integration Module for Cisco Physical Security Operations Manager* • *Cisco VSM 7.0 Integration Module for Cisco Physical Security Operations Manager* [add landing page link]	☐
Step 10	Install the PSOM client.	See Chapter 3, "Installing PSOM"	☐

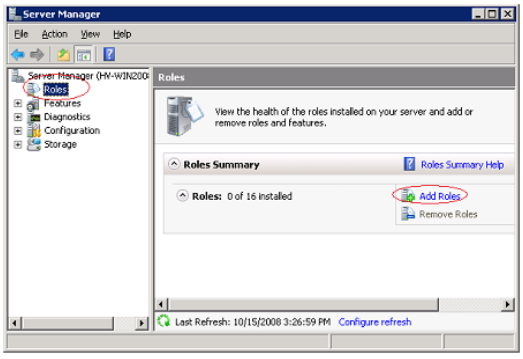
Preparing a Windows 2008 R2 X64 machine for PSOM

Note These instructions assume a blank Windows 2008 R2 X64 installation has taken place. The Windows 2008 R2 X64 setup disk is required.

Step 1 Install Server Roles:

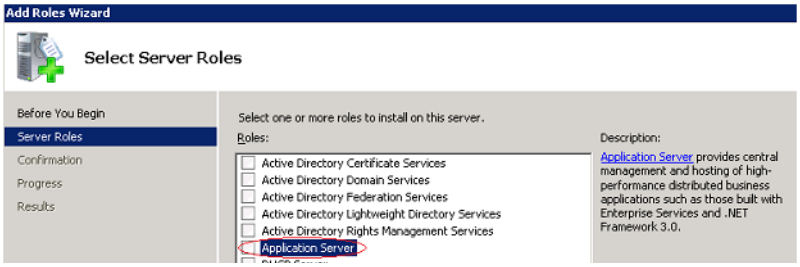
a. Select **Start > Administrative Tools > Server Manager**.

b. Click **Roles** and then click **Add Roles**.

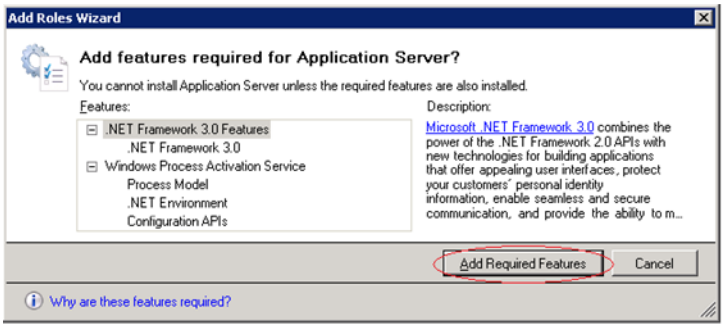


c. On the Before you Begin screen, click **Next**.

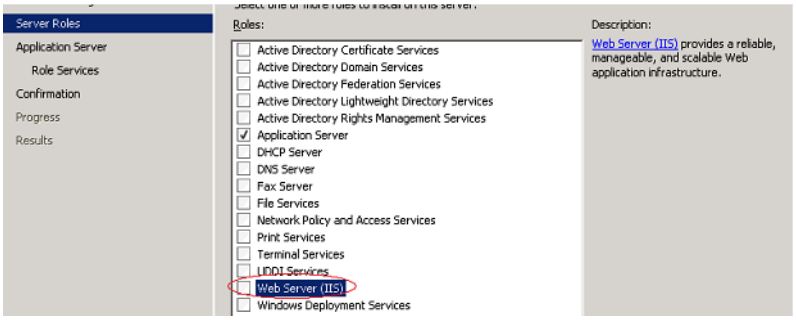
d. On the Select Server Roles screen, select **Application Server**.



e. At the popup window, click **Add Required Features**.

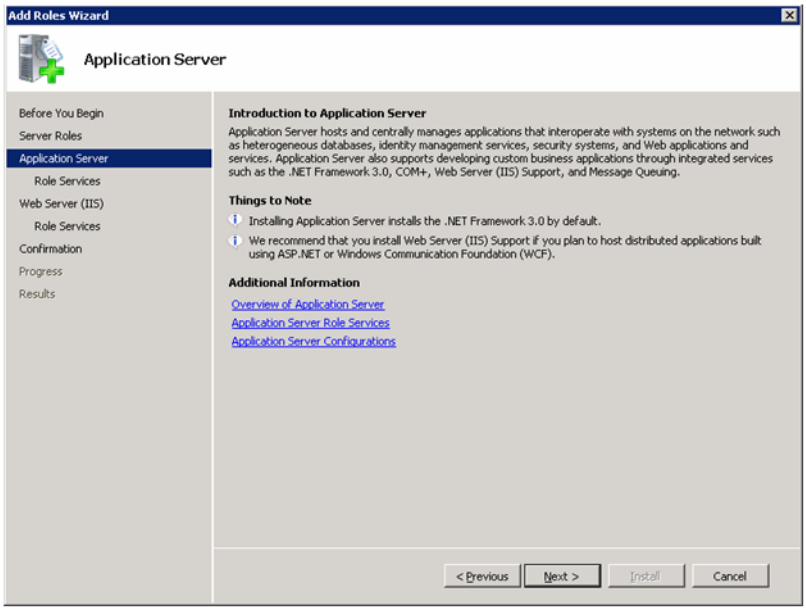


f. On the Select Server Roles screen, select **Web Server(IIS)**.



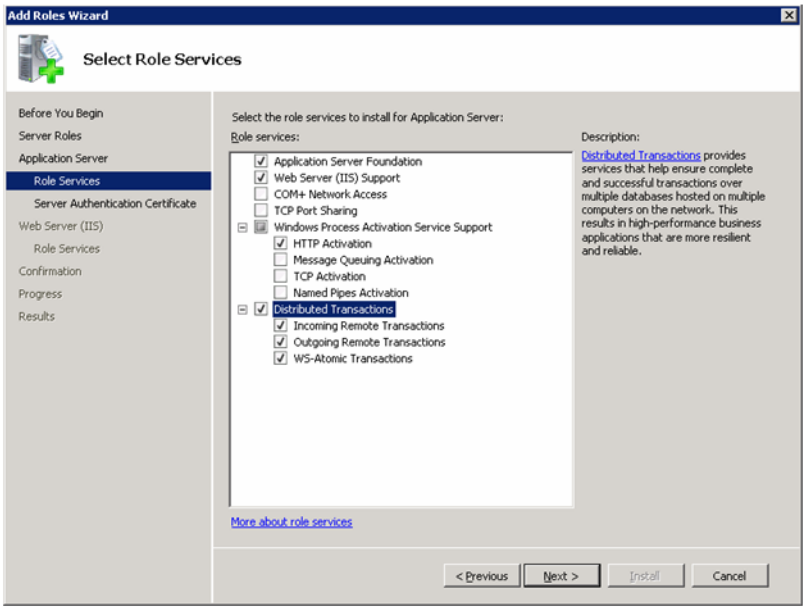
Step 2 Click **Next**.

Step 3 On the Application Server screen, click **Next**.

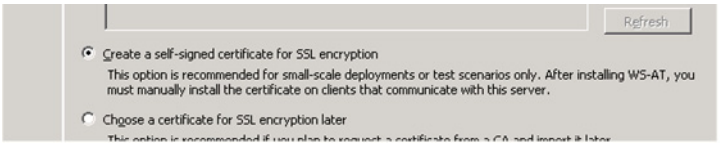


Step 4 Select the required role services when prompted to Add Required Services: Application Server Foundation, Web Server (IIS) Support, Distributed Transactions.

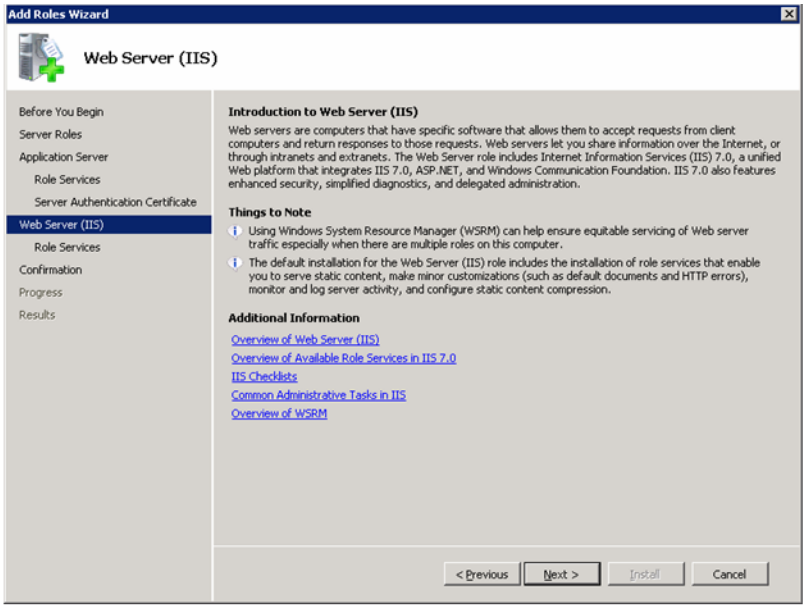
Step 5 Click **Next**.



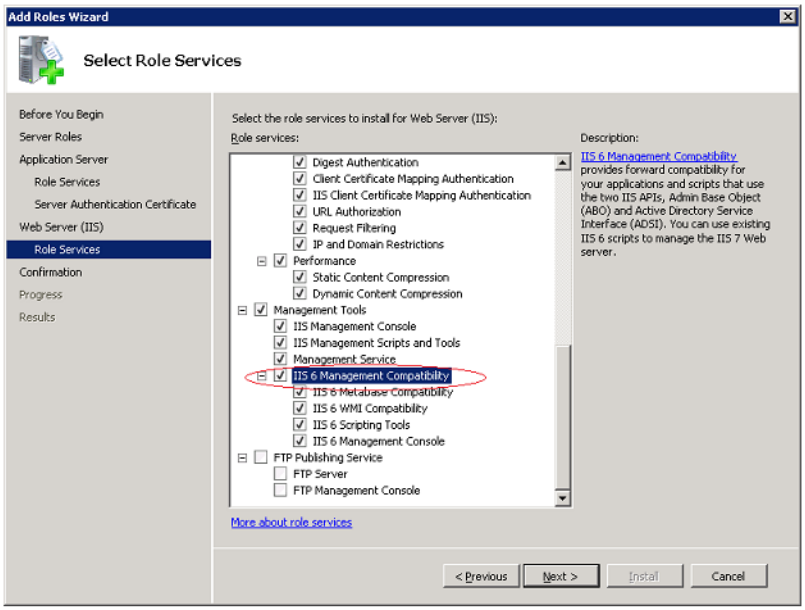
Step 6 On the Server Authentication Certificate for SSL Encryption screen choose, the **Create a self-signed certificate for SSL encryption** option and click **Next**.



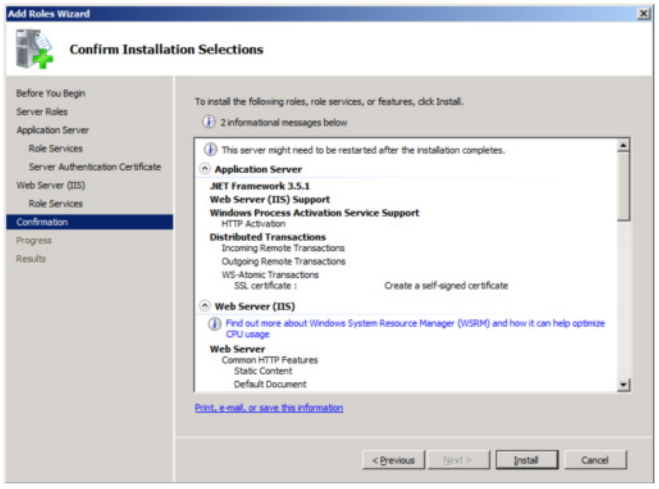
Step 7 On the Web Server (IIS) screen, click **Next**.



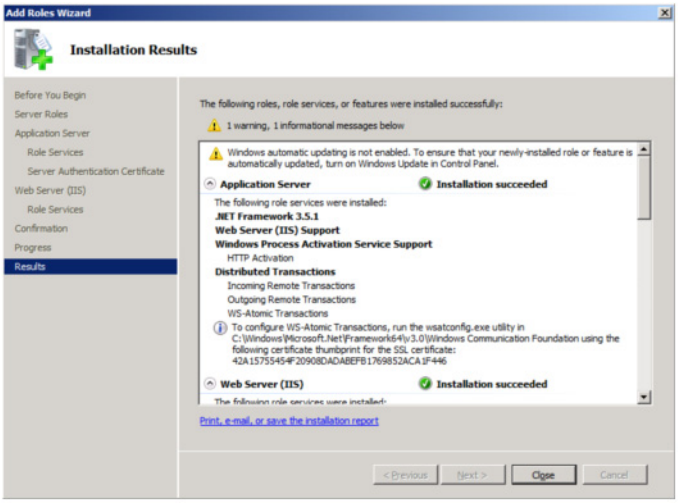
Step 8 On the Select Role Services screen, scroll down and select **IIS 6 Management Compatibility**, then click **Next**.



Step 9 On the Confirm Installation Selections screen, click **Install**.



The Application Server Role and IIS Server Role is now being initialized.



Step 10 Windows 2008 R2 Server is now prepped to host PSOM Services. Click **Close**.

Verifying/Installing IIS 6 Management Compatibility

Step 1 To determine whether IIS 6 Management Compatibility is installed, take these actions:

a. Select **Start > Administrative Tools > Server Manager**.

b. In the Navigation pane, expand Roles and look at Roles Summary.

c. Scroll to the bottom of the window and, under Installed Role Services for Web Server, verify whether IIS 6.0 Management Capability Components are installed.

If IIS 6.0 Management Capability Components are not installed, continue with this procedure.

Step 2 Select **Start > Administrative Tools > Server Manager**.

Step 3 In the navigation pane, expand Roles, right-click **Web Server (IIS)**, and then click **Add Role Services**.

Step 4 In the Select Role Services area, scroll to **IIS 6 Management Capability**.

Step 5 Check these check boxes:

- IIS 6 Metabase Compatibility
- IIS 6 WMI Compatibility
- IIS 6 Management Console

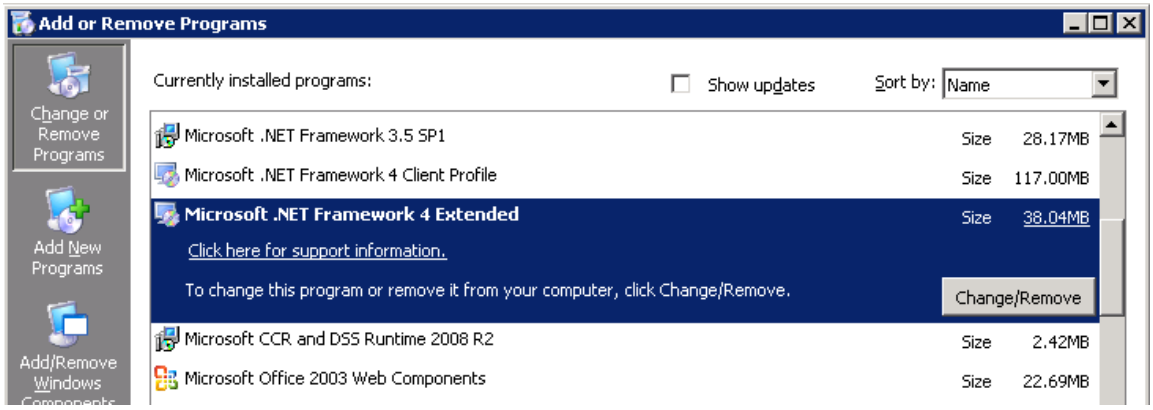
Step 6 Click **Next**.

Step 7 Click **Install**.

Step 8 Click **Close**.

Verifying that .NET Framework is Installed

All PSOM 6.1 software requires .NET 4.0 SP1. You can check to see if you already have the correct version of .NET Framework installed by clicking **Start** on your Windows desktop, choosing **Control Panel**, and then selecting **Programs and Features**. When that window appears, scroll through the list of applications. If you see **Microsoft .NET Framework 4 (Extended)** listed, the correct version is already installed and you do not need to install it again.



If you do not have Microsoft .NET Framework 4, you can download it here:
http://www.microsoft.com/download/en/details.aspx?id=17851

To obtain Microsoft .NET Framework 4 SP1, you can download it here:
http://www.microsoft.com/download/en/details.aspx?id=27757

Installing SQL Server 2008 R2

Note When installing Microsoft SQL Server 2008 (or Microsoft SQL Server 2008 R2) for use with PSOM there are three main settings that must be configured:

- The security mode must be set to Windows authentication mode
- The collation must be case insensitive (default)

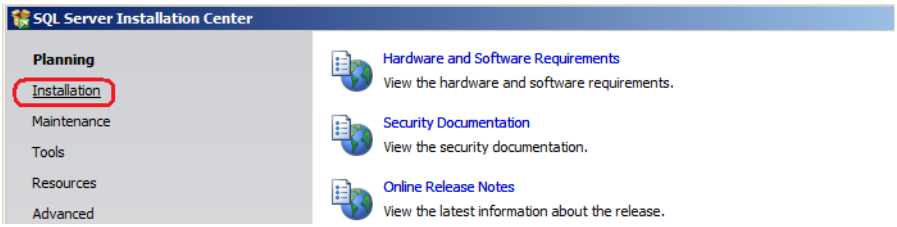
- SQL Server and SQL Server Agent must be automatically started when the Windows server machine is started

To install SQL Server 2008 R2:

Procedure

Step 1 Launch the installation of SQL Server 2008 R2.

Step 2 Examine the Requirements and Release Note Documentation section, then click **Installation**.



Step 3 At the Installation window, click **Installation or add features to an existing installation** to start the SQL Server installation.

Step 4 Install any necessary software in the Setup Support Rules window and click **OK**.

Step 5 Enter the product key and click **Next**.

Step 6 Accept the license terms and click **Next**.

Step 7 At the Setup Support Files window, click **Install**.

Step 8 When the installation completes, click Next.

Step 9 At the Setup Role window, select **SQL Server Feature Installation**.

Step 10 On the Feature Selection window, select **Database Engine Services**, **Client Tools Connectivity**, **Client Tools Backwards Compatibility** and **Management Tools – Complete**, and then click **Next**.

Step 11 On the Instance Configuration window select **Default instance** and accept the default directory unless a default SQL Server has already been installed. If a default SQL Server has already been installed then create a *named instance* and provide the default directory path.

Step 12 Review information on the Disk Space Requirements window and click **Next**.

Step 13 On the Server Configuration window, click the **Service Accounts** tab.

a. Enter **NT AUTHORITY\SYSTEM** in the Account Name field for both **SQL Server Agent** and **SQL Server Database Engine**.

b. Select **Automatic** from the Startup Type field for both **SQL Server Agent** and **SQL Server Database Engine**.

Step 14 Click the **Collation** tab in the Server Configuration window, then click **Customize** and select **SQL_Latin1_General_CP1_CI_AS** and click **Next**.

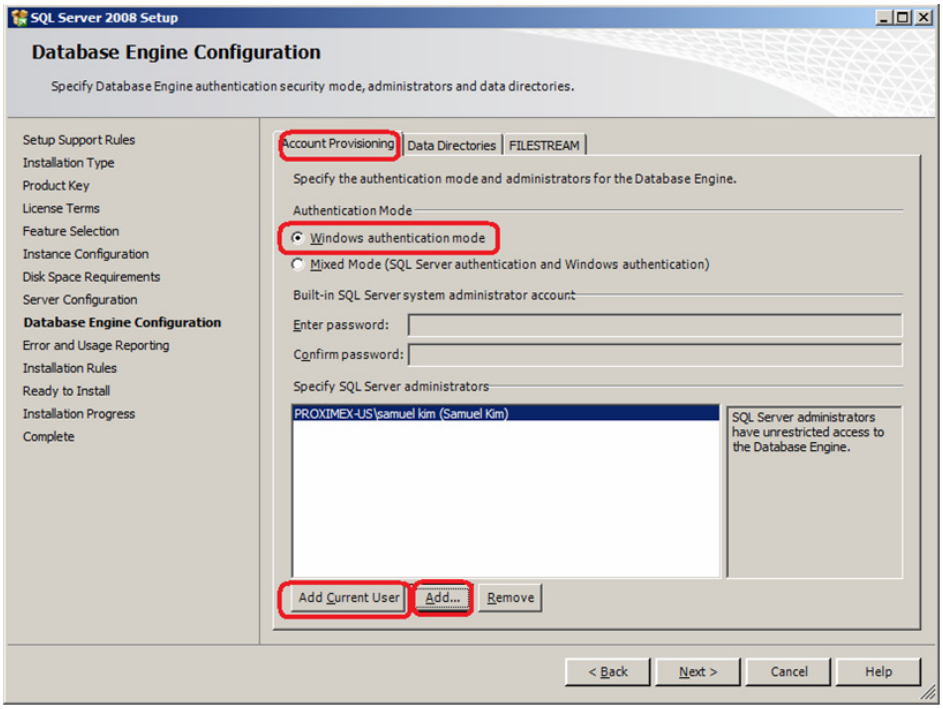
Step 15 In the Database Engine Configuration screen, click the **Account Provisioning** tab.

a. Select the **Windows authentication mode** option.

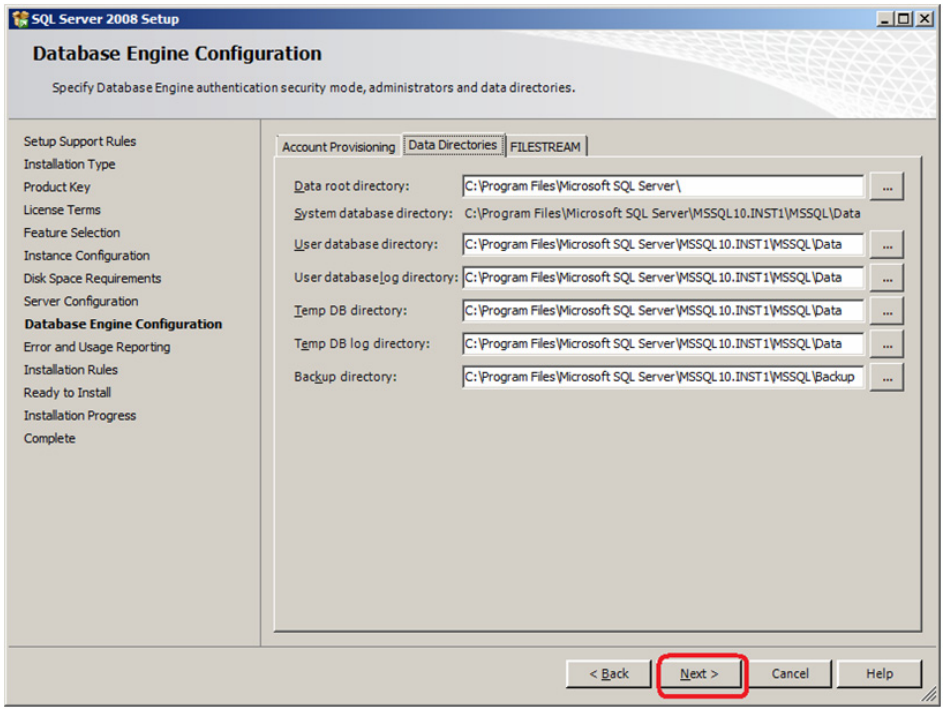
b. Click **Add Current User** to add the current user to SQL Server sysadmin.

c. Click **Add…** to include additional Windows NT users (or groups) in the sysadmin group.

Note It is recommended that you add the local Administrators group to the sysadmin group.



Step 16 If you have multiple disks, click the **Data Directories** tab on the Database Engine Configuration window. From this tab you can select appropriate directories.



Note You may have higher database performance if the Temp DB directory and Temp DB log directory are on different a drive than the User database directory.

Step 17 Click **Next**.

Step 18 Select the appropriate level of reporting from the Error and Usage Reporting window and click **Next**.

Step 19 Click **Next** at the Installation Rules window.

Step 20 Click **Install** at the Ready to Install window.

Step 21 Click **Next** at the Installation Progress window.

Step 22 Click **Close** at the Complete window.

Step 23 Install Server Pack 1 for SQL Server 2008.

a. Launch the installation, click **Next** at the Welcome screen, and accept licensing terms and click **Next**.

b. On the Select Features window, click **Select All** and click **Next**.

c. On the Check Files In Use window, wait for the check to complete and click **Next**. You can click **Stop Check** if you want to halt the verification process.

d. On the Ready to Update window, click **Update**.

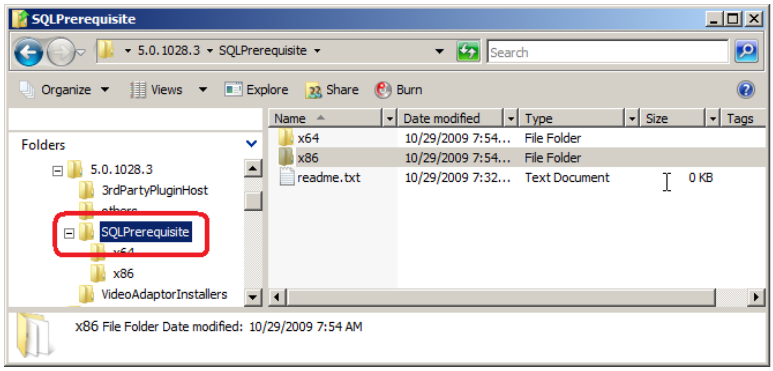
e. Click **Next** when the update is complete.

f. Click **Close** to finish the update.

Prerequisite Installation for PSOM Web Service and Connector Web Service

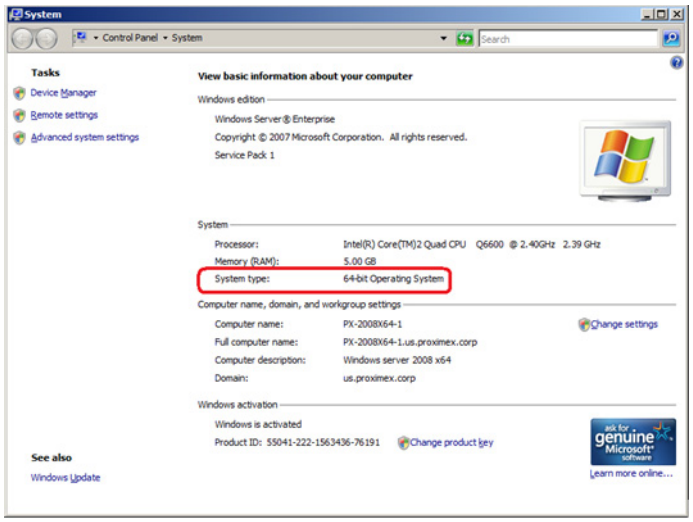
For Integration Module wizards to function properly, additional Microsoft-based programs need to be installed.

These Microsoft updates are included in the SQL Prerequisite folder on the PSOM setup disk and should be installed before the PSOM Web Service or Connector Web Service are installed. The subdirectory (x64) contains the necessary installation for the 64bit(x64) Windows operating systems.

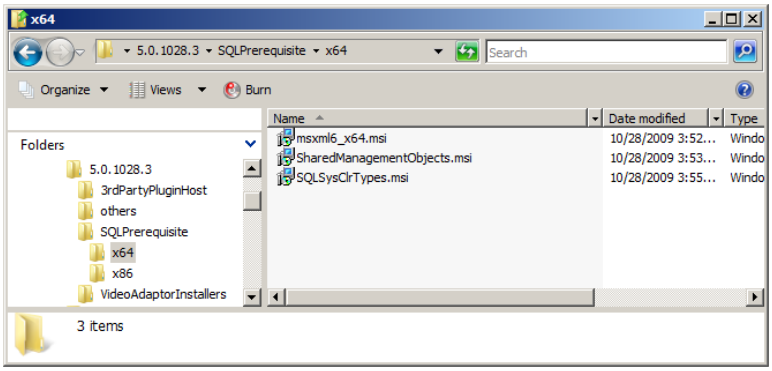


To verify your operating system, select **Start > Computer**, right-click and select **Properties**. Examine the Properties window to ensure that you are operating a 64-bit Windows 2008 operating system. The next example shows the Properties window for a 64-bit Windows operating system.

Execute the files in the x64 directory.



The following example shows the contents of the x64 directory.



The following table lists the files and the order in which they should be executed.

Table 2-2

File	Description
msxml6_x64.msi	Search for Microsoft Core XML Services (MSXML) 6.0.
SQLSysClrTypes.msi	Search for Microsoft SQL Server System CLR Types.
SharedManagementObjects.msi	Search for Microsoft SQL Server 2008 Management Objects.

Changing Application and System Log File Settings

Logging information for the PSOM Services nd the Microsoft SOAP Toolkit is sent to the Windows Event Viewer. In the Application Log you will find information about the status of the service (during startup and shutdown), and warnings or errors if something goes wrong. The default Application Log size may be too small for your application. The default size of the System Log might also be too small. To avoid errors, you should increase the size of both logs to 5012 KB. In addition, the **Overwrite as Needed** option is recommended to insure that no recent events are lost.

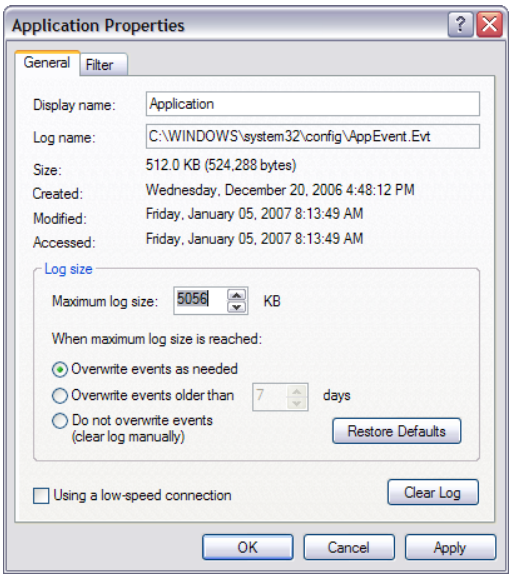
Note These steps should be performed on the Windows 2008R2 (x64 only) machine that is running PSOM Services.

To change Application and System log file settings:

Step 1 Use the **Run** command in the **Start** menu to launch the **Event Viewer** by running **eventvwr.msc** or by running the command **eventvwr.exe** from a **cmd** window.

Step 2 Select **Application** from the treeview.

Step 3 Select **Properties** from the **Action** menu.



Step 4 Change the **Maximum log size** to fit your environment. A log of 5012 KB is recommended.

Step 5 Select **Overwrite events as needed** option.

Step 6 Click **OK**.

Step 7 Repeat for the System log except select **System** from the treeview in the Event Viewer.

CHAPTER 3

Installing PSOM

If you are installing PSOM for the first time, follow the instructions in this chapter to install the PSOM Services and PSOM Consoles.

If you are upgrading from a previous release of PSOM, see Chapter 2, "Upgrading PSOM.".

This document includes these topics:

Installing PSOM

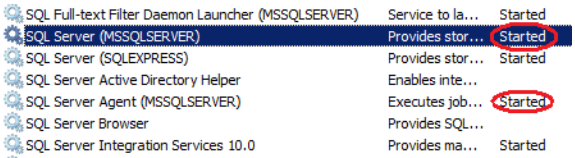
This section covers the steps, in the appropriate order, for installing PSOM.

To install PSOM, follow these steps:

Procedure

Step 1 Copy over the file to locally accessible drive.

Step 2 Verify that SQL Server and SQL Server Agent are started by selecting **Start > Administrative Tools > Services** and locating the SQL Server (MSSQLSERVER) and SQL Server Agent (MSSQLSERVER) in the list.



Step 3 Install PSOM Repository. See the "Installing PSOM Repository" section on page 3-2.

Step 4 Install PSOM Web Service. Se the "Installing PSOM Web Service" section on page 3-4.

Step 5 Install Connector Web Service. See the "Installing the Connector Web Service" section on page 3-17

Step 6 Install PSOM Integration Modules. See documentation for the specific Integration Modules you are using.

Step 7 Install PSOM Services. See the "Installing PSOM Services" section on page 3-8.

Step 8 Install PSOM Consoles. See the "Installing PSOM Consoles" section on page 3-23.

Step 9 Install PSOM User Services. See the "Installing PSOM User Services" section on page 3-24.

Step 10 Install the help systems for the Operation Console and Administration Console by double-clicking the PxDocSetup.msi files. The help systems must be installed on the machine where PxWebServiceSetup.msi was installed. Accept all default settings and proceed through installation. Click **Close** at the end.

Installing PSOM Repository

To install PSOM Repository, follow these steps:

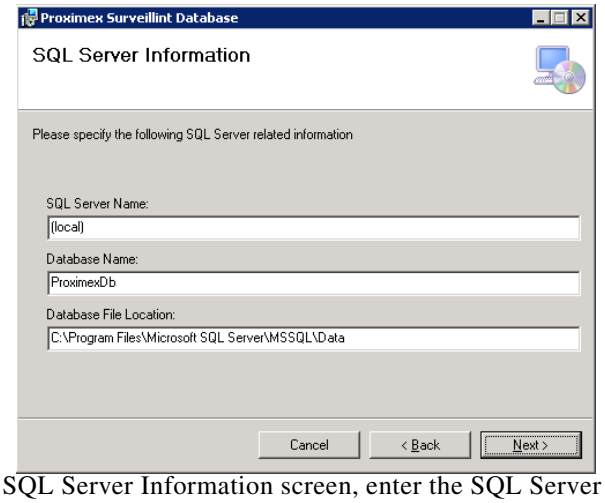
Procedure

Step 1 Double-click the **PxDatabaseSetup.msi** file.

Note If you're running in a clustered environment, make sure that you're running the setup in the active machine node.

Step 2 Click **Next**.

Step 3 Click **I agree** for the license agreement and click **Next**.

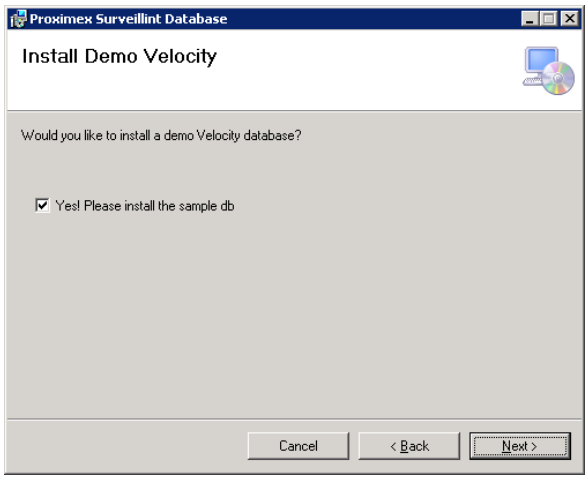


Step 4 On the SQL Server Information screen, enter the SQL Server Name\Instance Name in the **SQL Server Name** field. For a cluster environment, enter the Virtual SQL Server\Instance Name.

Step 5 Do not change the database name in the **Database Name** field.

Step 6 Enter the directory where you want database files stored in the **Database File Location** field. Make sure that this directory already exists in the Windows server directory structure before you click **Next**.

Step 7 Click **Next**.

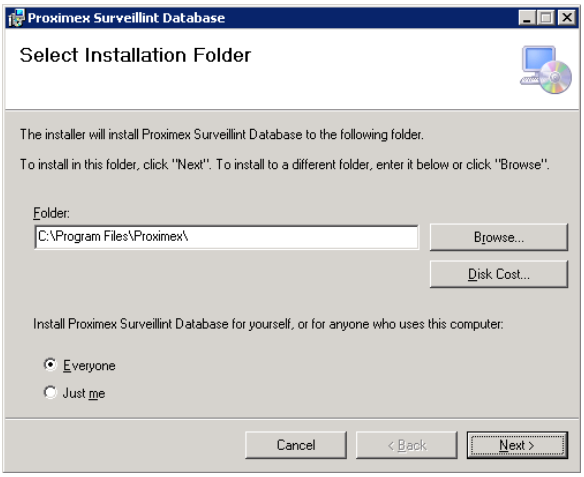


Step 8 If you want to install the sample database, check the **Yes!** option. If you choose to install the demo database it will be created in the same directory as was specified for ProximexDB.

Step 9 Determine whether you want a new database installation, or if you want to upgrade an existing (5.1 version) database installation. Selecting **New** overwrites the existing database installation. Selecting **Upgrade** preserves your PSOM configurations (sensors, areas, zones, rules, etc.) while upgrading it to the latest database schema.

Note Upgrading will upgrade database schema, business logic and alert tasks to 6.1.

Step 10 Click **Next**.



Step 11 Click **Next** to accept the default installation directory.

Step 12 Click **Next** on the Confirm Installation screen to continue with installation.

Note You can verify installation by opening SQL Server Management Studio, connecting to SQL Server using the sa username (sa password), and validating that the user PROXIMEX_SYS has been created. Also, execute this command:

```
use ProximexDb
go
```

Select DATEADD(hour, DATEDIFF(hour, GETUTCDATE(), GETDATE()), LUTime) InstallTime, * From PxVersion
go

Validate that the InstallTime column as outlined above matches the time that the installation took place.

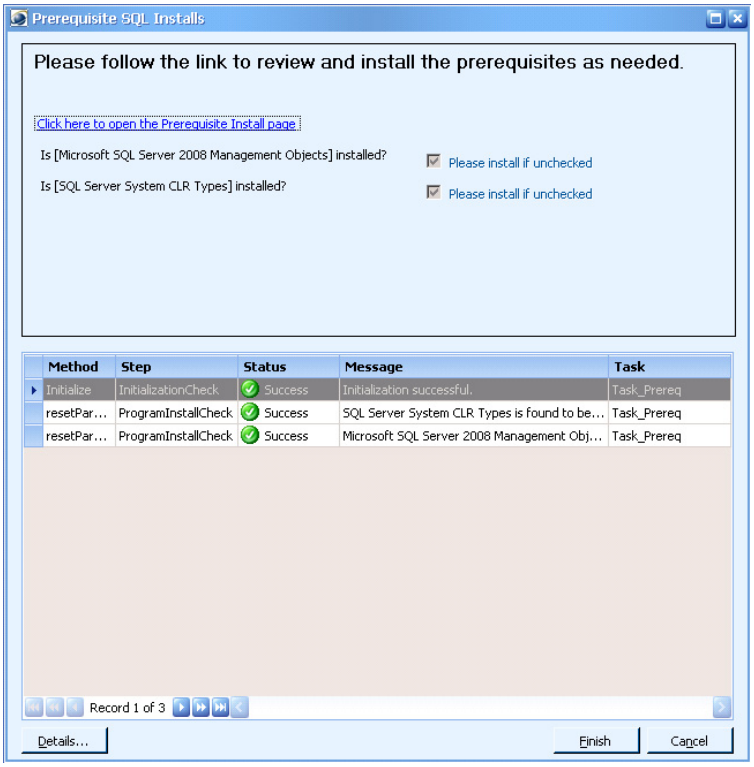
Installing PSOM Web Service

To install PSOM Web Service, follow these steps:

Procedure

Step 1 Install the Wizard Prerequisite Check by double-clicking the **PxWizardPrereq.msi** file.

The following window appears after the installation completes.



If the **Please install if unchecked** options are greyed, then the required components have already been installed on the machine. In this case, click **Finish** to finalize the installation.

If these options are not greyed, then click the link to open the Prerequisite Install page and view detailed information about Microsoft components that need to be installed on this machine.

Step 2 Right-click the **PxWebServiceSetup.bat** file and select **Run as administrator**.

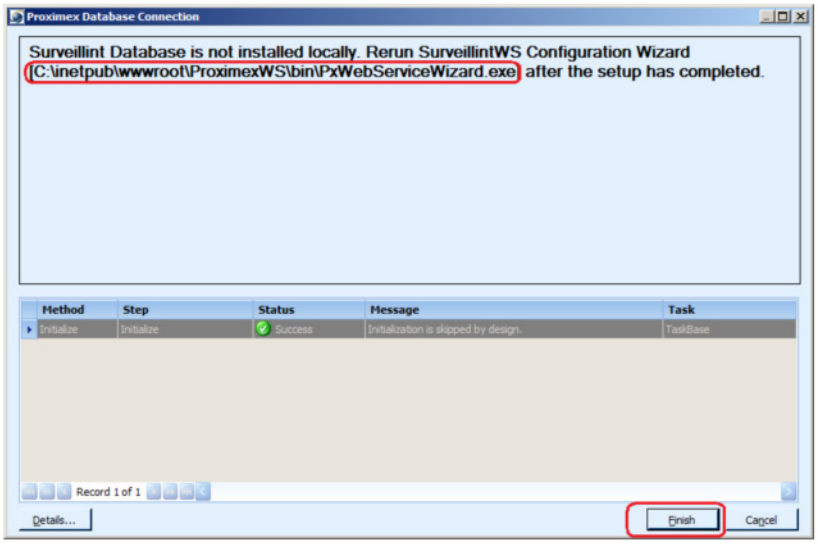
Step 3 Click **Next**.

Step 4 Accept the license agreement and click **Next**.

Step 5 In the Select Installation Address window, leave the default values and click **Next**.

Step 6 Click **Next** in the Confirm Installation window.

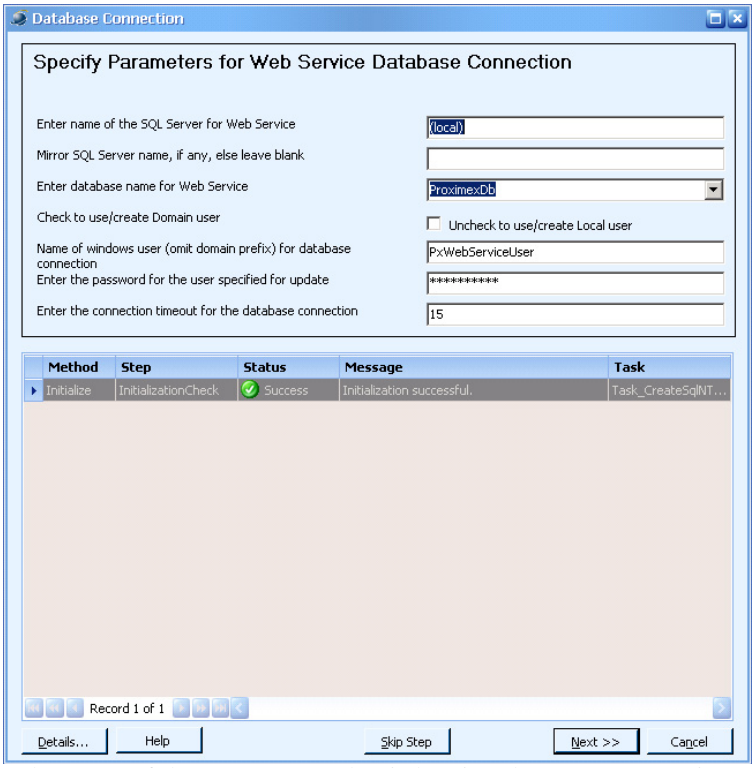
Step 7 If the PSOM Repository (ProximexDB) is not installed on this machine, the following window appears.



Click **Finish** if this window appears, and click **Finish** again. Then double-click the PxWebServiceWizard.exe file located in the C:\Inetpub\wwwroot\ProximexWS\Bin\PxWebService.exe directory. Then rerun the PSOM Web Service installation (PxWebServiceSetup.msi file).

See the "Changing the Configuration of the PSOM Web Service" section in *Administering Cisco Physical Security Operations Manager* for details.

Step 8 If the PSOM Repository (ProximexDB) is installed on this machine, the following window appears.



Step 9 Enter the name of the SQL Server that is hosting the PSOM Repository in the **Enter name of the SQL Server for Web Service** field. Normally this is the local machine name unless the PSOM Repository is located on a different server.

Step 10 If you are using a mirrored database, enter the name of the mirrored SQL Server in the **Mirror SQL Server name** field. Otherwise, leave this field blank.

Step 11 Leave the value of the **Enter database name for Web Service** field set to ProximexDb unless you have customized the name of the PSOM Repository.

Step 12 If you are using a domain Windows user for the connection to PSOM Repository, select the **Check to use/create Domain User** option. Otherwise, leave this option unchecked to use a local Windows user for access to the Repository.

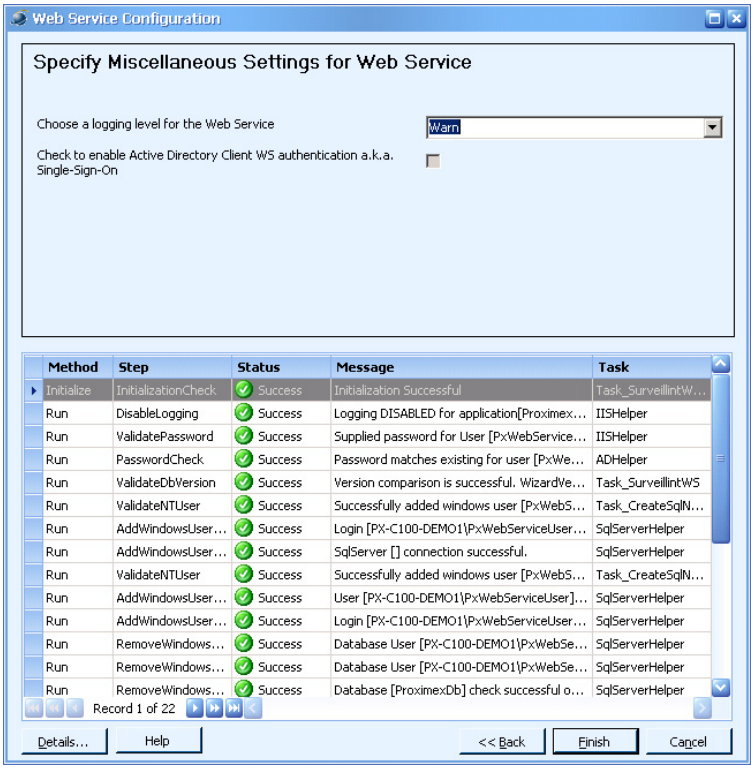
Note If you do not have permission to create a local or domain Windows user, this step will fail. You must then create the user account manually and re-run this wizard.

Step 13 Enter the name of the local or domain Windows user to be used for accessing PSOM Repository in the **Name of windows user for database connection** field. Do not include the domain name or machine name. The default value is PxWebServiceUser.

Step 14 In the **Enter the password for the user specified for update** field, enter the corresponding password.

Step 15 In the **Enter the connection timeout for the database connection** field, enter the number of seconds to wait for a response from the database. The default is 30 seconds.

Step 16 Click **Next**. The following window appears.

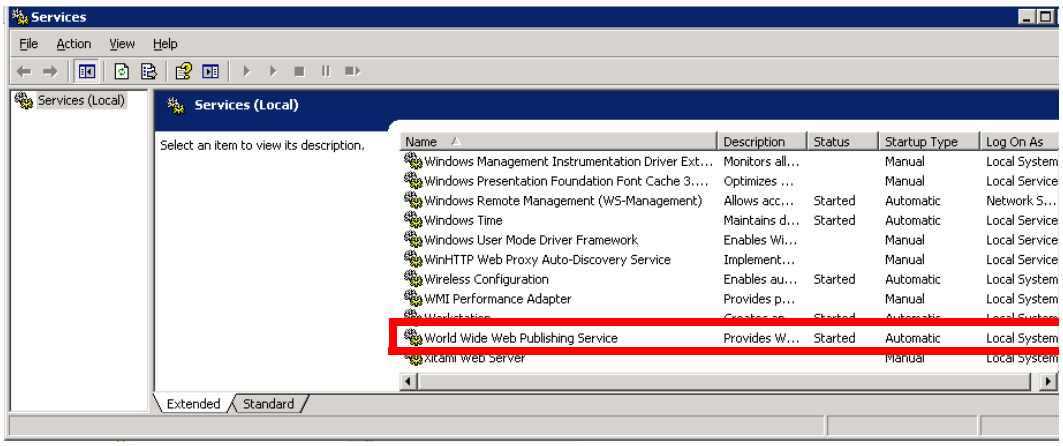


Step 17 Select the desired level of logging for the PSOM Web Service from the **Choose a logging level for the Web Service** field. Choices include: **Debug**, **Info**, **Warn**, **Error**, or **Fatal**.

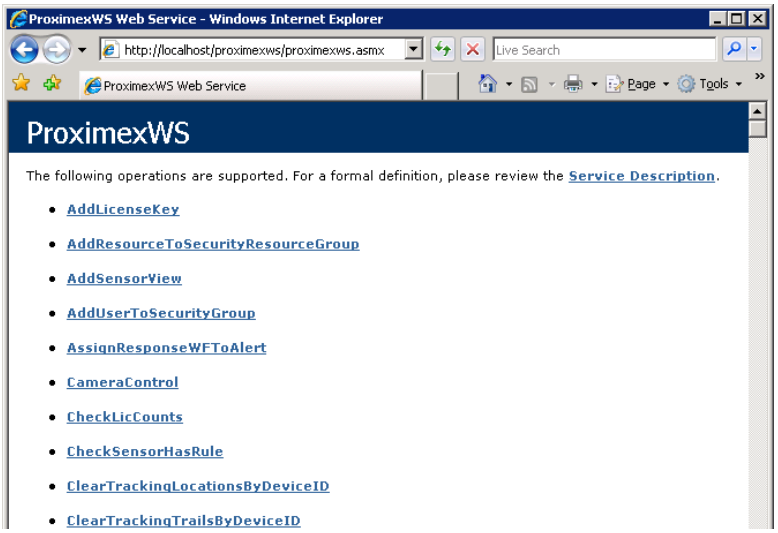
Step 18 If you want to use Active Directory for user authentication, select the **Check to enable Active Directory Client WS authentication** option. By default, Active Directory is not used for user authentication by PSOM or the Web Service.

Step 19 Click **Finish**, click **OK** when prompted, and click **Close** at the final screen.

Step 20 If you want to verify installation, open the Service Manager by clicking **Start > Administrative Tools > Services**, and verify that the World Wide Web Publishing Service is running.



Step 21 Open Internet Explorer or other web browser and navigate to this url: http://localhost/proximexws/proximexws.asmx.



If you do not see this page, the ASP.NET has not been correctly set up on the server. Make sure to allow **Anonymous Updates** and confirm that the .NET framework has been **Allowed** to function in IIS.

Installing PSOM Services

Note You must be a member of the local Administrators group to launch Services Configuration. In fact, it is recommended that you create a dedicated Windows or Active Directory Domain account to run the installation of PSOM Services instead of using the "Local System" account.

To install PSOM Services:, follow these steps:

Procedure

Step 1 Double-click the PxManagedServicesSetup.msi file.

Note Microsoft PowerShell 2.0 is required to install PSOM Services.

The Welcome window appears.

Step 2 Click **Next** and click **Next** again to accept the license agreement.

The Custom Setup window appears.

Step 3 In the Custom Setup window, choose individual service components to install. By default, all service components are selected.

Step 4 Accept the default installation folder and click **Next**.

Step 5 In the Ready to Install window, click **Install** to begin installation.

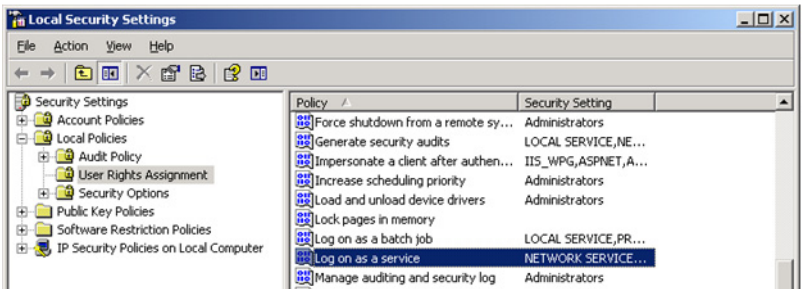
The Services Configuration window appears

In the Services account information area, select **Local System Account** to use the default account to run PSOM Services.

If you want to specify a different user account, make sure the account meets the following criteria:

- Belongs to the local Administrators group
- Has permission to SQL Server database through Integrated Windows Security
- Has permission to Run as service

To ensure the account has the Run as service permission, you need to launch the Local Security Settings window, select **Local Policies > User Rights Assignment**, and double-click **Log on as a service**.



When specifying a user account, select **Specific User Account** and enter:

- The name of the user account on the Windows Server that PSOM Services will use to perform administrative functions in the **Service Account** field.
- The password for that service account in the **Password** field.

Step 6 In the Services Configuration window, click **Next** or **2 – Connections** to configure connections to the PSOM Repository and PSOM Web Service. In the **Database** tab of the Configure Connections area:

- The **Database Server** field contains localhost unless you installed PSOM Repository on a different machine in the network. In this case, enter the IP address or server name of the machine where PSOM Repository is installed.
- The **Database** field contains ProximexDb, unless there is a reason to change the name of the PSOM Repository.
- The **Port** field contains the port number under which the Repository runs.
- The **Default Timeout** field contains the number of seconds the Managed Services will wait for a response from the PSOM Repository.
- If you are using a mirrored database, click **Mirror DB server** and enter the IP address or server name of the machine where the mirrored database resides.
- If you want to use Microsoft SQL Server authentication for the PSOM Repository, check the **Use SQL Authentication** option. Then enter the SQL user login and password in the fields provided.

  PSOM Services can use both the Integrated Security mode and SQL Server security mode for connections. Ensure that SQL Server allows the connection mode you specified.

Note When you click **Test Connection** on the **Database** tab, your current Windows account is used to authenticate the SQL Server and SQL database.

Step 7 Click the **Web Service** tab in the Configure Connections area. In this tab:

- The **WS Server** field contains localhost unless you installed PSOM Web Service on a different machine in the network. In this case, enter the IP address or server name of the machine where you installed PSOM Web Service.
- The **Service Port** field contains the port number at which the PSOM Web Service should listen for communications. The default is 80.
- If you are configuring redundant PSOM Web Services, check the **Secondary WS Server(s)** option and enter the IP addresses or server names of backup PSOM Web Services, separated by commas.
- If SSL (Secure Sockets Layer) is enabled for Web Services, check the **Secured Connection** option to make sure the Managed Services use SSL (HTTP over SSL) to connect to the PSOM Web Service. This setting applies to all configured PSOM Web Services.
- The **SysUser Password** field contains the administrative password for the machine where the PSOM Web Service is installed. To change the SysUser password, enter a new password and click **Set Password**. If you change the SysUser password, you must update all Managed Services and User Services to use the new password.

Note If SSL is configured, the only way to connect to PSOM components is via HTTPS. Therefore, all links need to be updated. For example:

Web Access URL—https://hostname/pxwebaccess
Connector Plugin Pages URL—https://localhost/PxConnectorWS/PluginPages/default.aspx

Further, when logging into PSOM Consoles, users must check the **Use HTTPS connection** option.

Click **Test Connection** to verify settings.

Step 8 Click the **Connector Web Service** tab in the Configure Connections area. In this tab:

- The **ConnectorWS Primary Server(s)** field contains localhost unless you installed PSOM Connector Web Service on a different machine in the network. In this case, click **Add Primary** and enter the IP address or server name of the machine where you installed PSOM Connector Web Service.
- If you have installed failover Connector Web Services, click **Add Secondary** and enter the IP address or server name of the machine where you installed the PSOM Connector Web Service in the New Server Location dialog.
- Specify the maximum number of times PSOM will attempt to connect to the primary Connector Web Service in the **Maximum Retry** field. After this, PSOM will either manually or automatically failover to secondary Connector Web Services.
- By default, PSOM is configured so that failover to a secondary Connector Web Service is performed manually. If you want failover to be performed automatically, uncheck the **Is Manual Fail Over** option.
- If you want to manually failover the Connector Web Service, click **Update Connector**. In the Select Fail Over ConnectorWS nodes dialog, select the primary node from which to failover, and the secondary node to which to failover. Click **OK**.

Step 9 Click **Next** or select **3 - Business Logic SDK** in the Services Configuration window.

If you have preconfigured business logic to deploy for PSOM, click **Browse** in the Business Logic SDK Deployment Configuration window and select the business logic SDK activity package (.zip extension) and click **Deploy**. If you want to reverse deployment for the SDK activity package, click **Undeploy**.

Step 10 Click **Next** or select **4 - Health Diagnostics** in the Services Configuration window. On the **General** tab of the Health Diagnostics Services Configuration window:

- The **Service Port** field contains the port number at which the Health Diagnostics Services should listen for communications. The default is 8011.
- Enter how often (in seconds) the Health Diagnostics Services should check the status of PSOM Services in the **Polling every x seconds** field.

Step 11 Click the **Agents** tab in the Health Diagnostics Services area and select an agent from the list to configure settings for it. You must click **Save** to store configuration changes for an agent before you can make the changes to the actual health monitoring agent.

Table 3-1 Health Diagnostics Agent Configuration

Agent	Configuration
Database Connectivity Agent	**Threshold for Database Connectivity Test** Enter the threshold (in milliseconds) that determines whether PSOM Services can connect with the PSOM Repository. The default is 60000 milliseconds.
IIS Worker Process Monitor Agent	**Upper Threshold for Total RAM Usage Test** Enter the threshold (in megabytes) that determines whether the maximum amount of RAM is being consumed by PSOM. The default is 4000 megabytes.
Managed Services: Services Availability Monitor Agents	**Interval for Services Offline Re-Notification** Enter the number of hours that should pass before another notification should be sent that services are offline. The default is 2 hours. **Include Availability Tests for User Services?** Select **True** if you want to provide service availability data collected by Managed Services to PSOM User Services.
Managed Services: Total RAM Usage Monitor Agents	**Threshold for Managed Services (Non Users Services) Total RAM Usage** Enter the maximum amount of RAM (in megabytes) that Managed Services can consume. The default is 6000 megabytes. **Threshold for User Services Total RAM Usage** Enter the maximum amount of RAM (in megabytes) that User Services can consume. The default is 2000 megabytes.
Monitoring Services: Alert Creation WS Response Time Monitor Agent	**Upper Threshold for WS: Alert Creation response time** Enter the maximum amount of time (in milliseconds) that should be allowed for alert creation. The default is 800 milliseconds.
Monitoring Services: Connector WS Monitor Agent	**Upper Threshold for Connector WS Plugin: Response Time** Enter the maximum amount of time (in milliseconds) that should be allowed for an Integration Module to respond. The default is 10000 milliseconds. **Upper Threshold for Connector WS Host: Response Time** Enter the maximum amount of time (in millisecond) that should be allowed for the Connector Web Service to respond. The default is 5000 milliseconds.

Managed Services: Services Availability Monitor Agents	**Interval for Services Offline Re-Notification** Enter the number of hours that should pass before another notification should be sent that services are offline. The default is 2 hours. **Include Availability Tests for User Services?** Select **True** if you want to provide service availability data collected by Managed Services to PSOM User Services.
Managed Services: Total RAM Usage Monitor Agents	**Threshold for Managed Services (Non Users Services) Total RAM Usage** Enter the maximum amount of RAM (in megabytes) that Managed Services can consume. The default is 6000 megabytes. **Threshold for User Services Total RAM Usage** Enter the maximum amount of RAM (in megabytes) that User Services can consume. The default is 2000 megabytes.
Monitoring Services: Alert Creation WS Response Time Monitor Agent	**Upper Threshold for WS: Alert Creation response time** Enter the maximum amount of time (in milliseconds) that should be allowed for alert creation. The default is 800 milliseconds.
Monitoring Services: Connector WS Monitor Agent	**Upper Threshold for Connector WS Plugin: Response Time** Enter the maximum amount of time (in milliseconds) that should be allowed for an Integration Module to respond. The default is 10000 milliseconds. **Upper Threshold for Connector WS Host: Response Time** Enter the maximum amount of time (in millisecond) that should be allowed for the Connector Web Service to respond. The default is 5000 milliseconds.

Table 3-1 Health Diagnostics Agent Configuration (continued)

Agent	Configuration
System: Physical Disk Usage Monitor Agents	**Threshold for Average Disk Queue Length** Enter the average number of requests to read data from the physical disk that will trigger an alarm. The default is 30000 requests. **Threshold for Average Disk Read Time** Enter the average disk read time (in milliseconds) that will trigger an alarm. The default is 5000ms. **Threshold for Average Disk Write Queue Length** Enter the average number of requests to write data to the physical disk that will trigger an alarm. The default is 30000 requests. **Threshold for Average Disk Write Time** Enter the average disk write time (in milliseconds) that will trigger an alarm. The default is 5000ms.
System: Remaining RAM Monitor Agent	**Lower Limit for Available System RAM Test** Enter the amount of RAM that must remain available (in megabytes); if the amount of RAM drops below this number, an alert is triggered.
Web Access: Connectivity Agent	**Enable Web Access Connectivity Test** Whether or not to enable a test of connectivity to Web Access.
Web Services: Connectivity Agent	**Threshold for Web Services Connectivity Test** Enter the maximum amount of time (in milliseconds) that is allowed for connections to the Web Service before an alert is issued. The default is 15000ms.

Step 12 Click the **Notifications** tab in the Health Diagnostics Services area and select a notification from the list to configure settings for it. Click **Save** to store configuration changes.

Table 3-2 Health Monitoring Notification Configuration

Agent	Configuration
Admin Alerts: Administrative Alert Dispatcher	**Create Admin Alert when severity is or more than:** Enter the severity level at which an administrative alert should be created in PSOM; for example, Warning.

Step 13 Click **Next** or select **5 - Bus Services** in the Services Configuration window and in the Bus Services Configuration area:

- The **Service Port** field contains the port number under which PSOM Services run.
- The **Response Workflow** tab provides an option for automatically starting Response Workflows upon alert dispatch; check the **Auto start Response Workflow after dispatch** option.
- The **Advanced** tab shows various polling interval settings at which PSOM Services are polled for general health (the **Services Health Check Polling Interval** field) as well as the interval at which PSOM polls for business logic after an alert has occurred (the **Post-Alert Business Logic Polling Interval**).

A shorter polling interval for the **Post-Alert Business Logic Polling Interval** can improve the response time for Alert Business Logic, but it will negatively impact CPU performance and database response on the host machine.

It is not recommended that you change settings on the **Advanced** tab unless directed by Customer Support.

The **Connector Registration Poll Interval** shows the interval at which the Bus Services updates commands and sensor type registration for connectors. A shorter polling interval will generally improve the response time for the system to discover and import new or updated sensor types and commands, but it will negatively impact the CPU performance and connector performance on the host machine.

- The **On-Demand** tab can be used to instantly refresh the Integration Module registrations cached by this instance of Bus Services. Integration Modules access third-party systems integrated with PSOM. Simply click the **Update Connector Registrations** button.

Step 14 Click **Next** or select **6 - Business Logic** in the Services Configuration window.

On the **General** tab of the Business Logic Services window, the **Service Port** field contains the port number under which PSOM Business Logic Core Services run.

On the **Advanced** tab of the Business Logic Services window, check the **Enable support for response business logic** if you want to allow PSOM to execute Response Business Logic.

Note It is not recommended that you change settings on the **Advanced** tab unless directed by Customer Support.

Step 15 Click **Next** or select **7 - Caching** in the Services Configuration window.

The PSOM Caching Service speeds up business logic execution by caching monitoring hierarchy and sensor map information.

In the Configure Caching Services area:

- The **General** tab allows you to specify the port number under which the PSOM Caching Service runs in the **Service Port** field, as well as the number of minutes that should pass before the Caching Service refreshes the cache in the **Cache refreshing interval** field. You can also limit the number of sensors that may be transferred at a time to protect system resources in the **Sensor transfer size** field (default is 500).
- The **On-Demand** tab allows you to instantly refresh the cache by clicking the **Refresh cache now** button. You can refresh the cache once installation is complete by relaunching the Services Configuration window.
- The **Advanced** tab enables you to resolve poor SQL Server query performance by increasing the timeout that the Caching Service uses for SQL commands in the **SQL Command Timeout** field.

Step 16 Click **Next** or select **8 - Collaboration Services** in the Services Configuration window and in the Collaboration Services Configuration area, configure a pair of ports that the Collaboration Services use for two-way (duplex) communication. The Duplex Port number is always the Service Port number plus one (+ 1):

- The **Service Port** field contains the port number under which PSOM Collaboration Services run.
- The **Duplex Port** field contains the duplex port number for the PSOM Collaboration Services. The service and duplex port numbers will both be used by the Collaboration Service.

Note If the Collaboration Services are not running, users will not be able to communicate via the Instant Messenger Console.

Step 17 Click **Next** or select **9 - Monitoring** in the Services Configuration window.

- On the **General** tab of the **Configure Monitoring Services** area:
- The **Service Port** field contains the port number under which PSOM Monitoring Services run.
- The **Event Source** field shows all the machines where an Event Source is installed. In this release, the only Event Source is the Video Alert Service. Click **Add** to define a new location, enter the IP address or server name in the dialog box and click **OK**.
- The **Polling Interval** field shows the interval (in milliseconds) at which the PSOM Monitoring Service will seek new events.

Note The minimum polling interval for monitoring services is 250 milliseconds. However, the recommended polling interval is 250-300 milliseconds or higher to avoid CPU contention within the host environment. If you have a dual core or quad core host environment, setting the polling interval to 250 milliseconds may be sufficient.

On the **Advanced** tab of the Configure Monitoring Services area:

- Check the **Discard events from sensors that are not imported** option if you do not want the Monitoring Service to report on events generated by entities that do not have corresponding sensors in PSOM. If you check this option, events from these sensors will not become alerts in PSOM. This option is disabled by default so PSOM can create sensors if necessary when sensors are not recognized from an incoming event.
- Check the **Enable querying incoming events on disk** option if you want incoming events polled from Connector Web Services and the Event Source services to be queued on disk before being processed by business logic. By default this option is enabled. If disabled, incoming events are queued in memory.

Note It is not recommended that you change settings on the **Advanced** tab unless directed by Customer Support.

On the **Ignore Status** tab of the Configure Monitoring Services area, you can specify the types of messages for different Sensors that can be ignored.

To add a message that can be ignored, click **Add**.

Enter the instance of an Integration Module for which to ignore status in the **Connector Instance** field, and then select the statuses that can be ignored. Click **OK** and the specification appears on the **Ignore Status** tab.

Step 18 Click **Next** or select **10 - Sensor Management** in the Services Configuration window and in the Sensor Management Services area:

- The **Service Port** field contains the port number under which PSOM Sensor Management Service runs.
- On the **Schedule** tab, select the date and time that the PSOM Sensor Management Service will begin running, and then choose how frequently it will run (hourly, daily, weekly, monthly) in the Type area. Specify the interval at which the service will execute as well.

- On the **Sync Source** tab:
  - For exporting Sensors defined in PSOM, control the performance of the export process by limiting the number of sensors exported at a time to the value specified in the **Export Sensors in chunks** field.
  - To control the performance of sensor synchronization, enter how much time to throttle (in milliseconds) in the **Throttle Time** field.
  - Check the **Automatically delete unmatched sensors** option if you want to remove any Sensors from PSOM that could not be identified in the external system by the Sensor Management Service.
  - Check the **Create sensor default hierarchy** option if you want the Sensor Management Service to create a Sensor hierarchy by default as Sensors are added to PSOM. Sensors will be grouped as specified in the custom parsing (defined on the **Custom Parser** tab) or in "Default Location."
  - Check the **Automatically append suffix to duplicate sensor names** option to append a number to the Sensor name if it already exists in the database.
  - Check the **Automatically generate sensor groups** option to create Sensor Groups with a prefix of "SG" in the name.
- On the **XML Source** tab on the **Sync Source** tab:
  - Check the **Automatically append suffix to duplicate sensor names** option to append a number to the Sensor name if it already exists in the database.
  - Check the **Automatically generate video sensor groups** option to create video Sensor Groups with a prefix of "VSG" in the name.
  - In the **Full path to folder with video sensor xml file(s)** field, enter the directory path to where you want XML sensor configuration files stored.
- On the **On-Demand** tab, you can run the sensor synchronization process on demand by clicking the **Sync Sensors Now** button.

  Note If sensor synchronization is already in progress, then the on-demand sync request will be ignored.

  When **Sync Sensors Now** is clicked, Sensors are created in "Default Location".

- On the **Custom Parser** tab, the default parser groups all newly discovered Sensors into one category: undesignated Monitoring Zone, undesignated Monitoring Area and undesignated Location. You can specify how each Sensor should be grouped by passing the enhanced parser an Excel spreadsheet that maps Sensor names to Monitoring Areas and Locations.

If you select **Default Parser** from the **Select Parser** field, the values in the other fields either are greyed out or ignored. The default parser groups all newly discovered Sensors into one category: undesignated Monitoring Zone, undesignated Monitoring Area, and undesignated Location.

If you want to perform custom parsing, see the "Specifying Custom Parsing" appendix of *Administering Cisco Physical Security Operations Manager* for details.

Step 19 Click **Next** or select **11 - Logs** in the Services Configuration window and in the Configure Log Files area:

- Select the level of events that should be maintained in the PSOM log files from the **Services Log Level** field.
- Enter the maximum size per log file (in bytes) in the **Log file size per log file** field.

- Enter the maximum number of log files to be maintained per PSOM Service in the Maximum number of log files per service field.

Note By default all services log file are located in the \Program Files\Cisco PSOM\Managed Services\Log directory.

Click **Finish**. The Apply change? prompt appears.

Step 20 Click **Apply changes and restart services**. The PSOM Monitoring Services restart and a confirmation window appears.

Step 21 Click **Finish**.

Step 22 If you want to verify installation, open the Service Manager by clicking **Start > Administrative Tools > Services**, and verify that the following services are running: Cisco PSOM Bus Services, Cisco PSOM Business Logic Core Services, Cisco PSOM Caching Services, Cisco PSOM Collaboration Services, Cisco PSOM Health Monitoring Services, Cisco PSOM Monitoring Logic Services, and Cisco PSOM Sensor Management Services.

After initial installation and configuration, you can modify Managed Services configuration by selecting **Start > All Programs > Cisco Physical Security Operations Manager Services > Services Configuration**.

Note Only one instance of the configuration wizard can run at a time. Therefore, close the wizard when finished making changes.

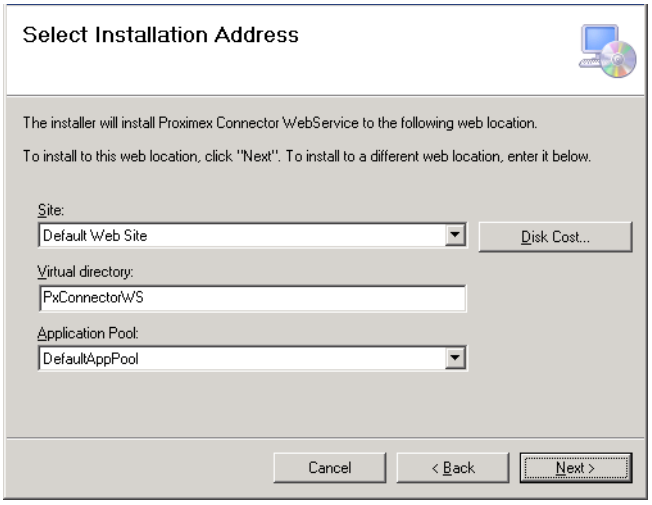
Installing the Connector Web Service

Procedure

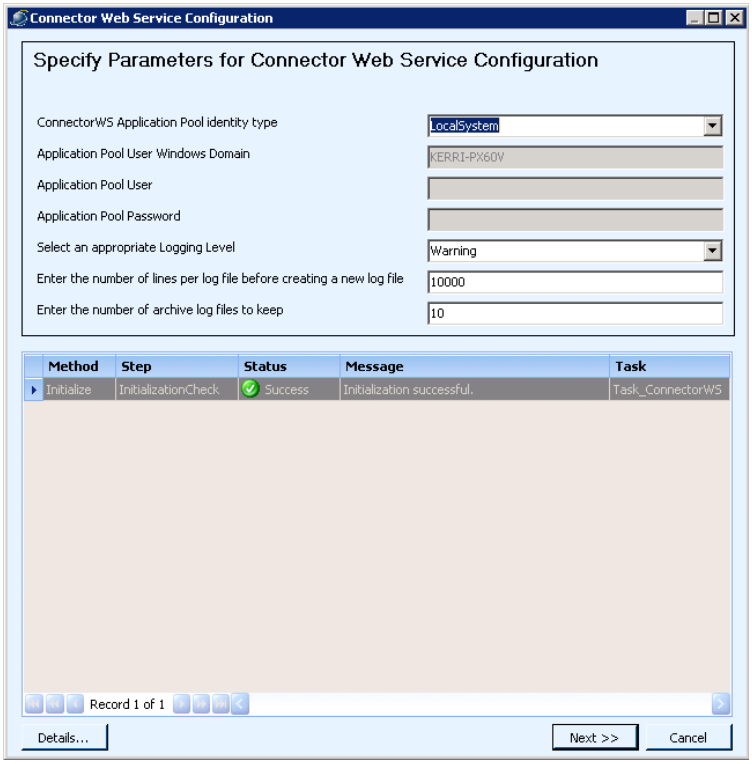
Step 1 Right-click the **PxConnectorWSSetup.bat** file and select **Run as administrator** to install the Connector Web Service.

a. Accept all default values.

b. In the Select Installation Address window, keep the defaults. Click **Next**.



The Connector Web Service Configuration window appears.



c. From the **ConnectorWS Application Pool identity type** field, choose the type of authentication to use for the Connector Web Service: **LocalSystem** or **WindowsUser**.

d. If you choose **WindowsUser**, complete these fields:

- In the **Application Pool Windows User Domain** field, enter the domain for the Windows user account that is being used by the Connector Web Service.
- In the **Application Pool User** field, enter the user account to be used by the Connector Web Service.

- In the **Application Pool Password** field, enter the password for the user.

e. Select the level of event messages to store in the Connector Web Service's log from the **Select an appropriate Logging Level** field: **Diagnostic**, **Informational**, **Warning**, **Severe**, or **Critical**.

f. In the **Enter the number of lines per log file before creating a new log file** field, enter the maximum number of lines to store in a log file before a new one must be created. The default number of lines is 10000.

g. In the **Enter the number of archive log files to keep** field, enter the maximum number of log files that can be stored by Connector Web Service. The default number of log files is 10.

h. Click **Next**. The Failover ConnectorWS Configuration screen appears. From this screen you can enable a backup Connector Web Service instance to quickly come online with all current Integration Module configurations in the event that the primary Connector Web Service is unavailable.

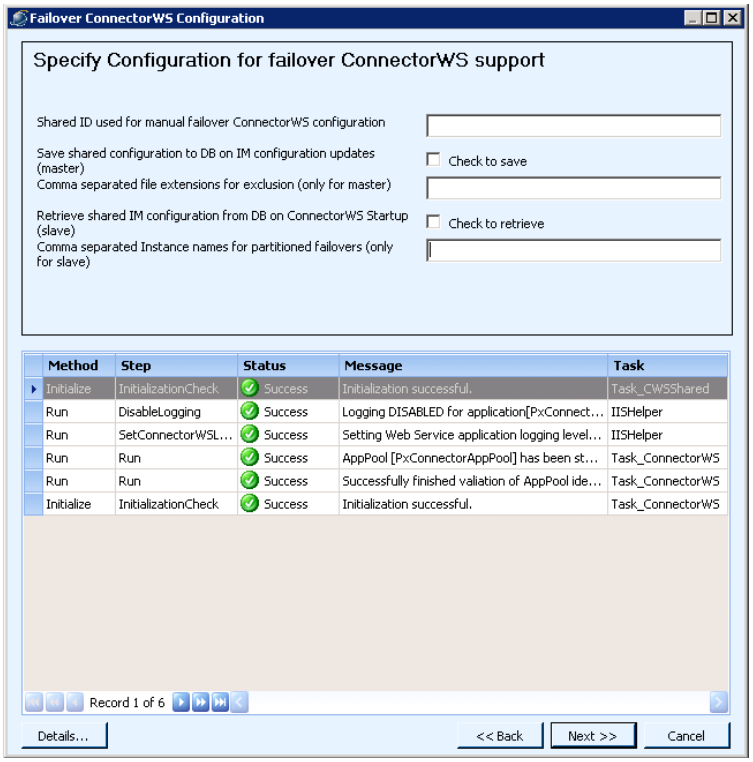
For example, consider a scenario with these Connector Web Service instances:

- MasterA—INST1 and INST2
- SlaveA_1—INST1
- SlaveA_2—INST2

Under normal circumstances, only MasterA should be running. If MasterA goes down, SlaveA_1 and SlaveA_2 are brought up by external sources to run INST1 and INST2, respectively.

When a Connector Web Service starts (for example, when the Plugin Pages are accessed or a Managed Service is using the Connector Web Service) it initializes itself using the configuration specified on the following screen.

If you do not want to configure a backup Connector Web Service for failover, then simply click **Next**.



i. Provide a name for the primary Connector Web Service configuration that can be stored in the PSOM Repository and accessed by a failover Connector Web Service in the **Shared ID used for manual failover ConnectorWS configuration** field. The primary Connector Web Service and any backup Connector Web Service instances must all use this same shared ID. If this field is left blank, the configuration will not be stored in the PSOM Repository.

j. If this Configuration Web Service should serve as the primary one, check the **Save shared configuration to DB on IM configuration updates** option. The configuration for this primary Connector Web Service will be saved to the PSOM Repository.

   When this option is checked, any changes to files under PxConnectorWS\App_Data (such as configuration of new Integration Modules, removal or updates of Integration Module instances, or any other changes to subdirectories under App_Data) will be saved to the PSOM Repository by PSOM Web Service.

k. If you do not want to backup certain configuration files, enter the file extensions for the files you do not want to backup to the PSOM Repository, separated by commas, in the **Comma separated file extensions for exclusion (only for master)** field.

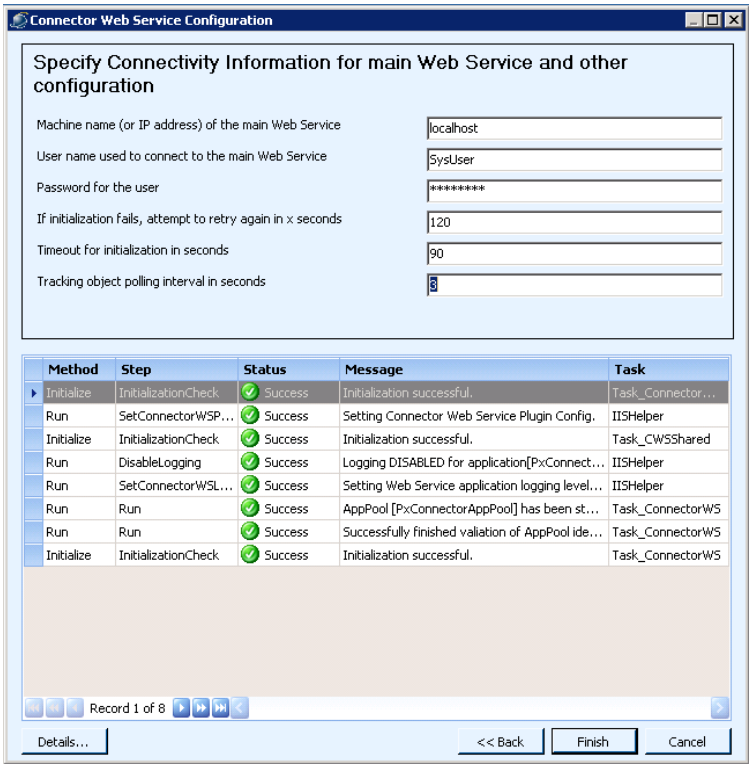
l. If this Configuration Web Service should serve as a backup one, check the **Retrieve shared IM configuration from DB on ConnectorWS startup** option. The configuration for this Connector Web Service will be retrieved from the PSOM Repository using the Shared ID provided.

m. If you only want to retrieve certain configuration files (for example for certain Integration Modules), enter the instance names of the Integration Modules you want to retrieve from PSOM Repository, separated by commas, in the **Comma separated Instance names for partitioned failovers** field. Only related files from PxConnectorWS\App_Data will be retrieved from PSOM Repository when the Connector Web Service is restarted.

   Leave this field blank to retrieve all configuration information stored for the primary Connector Web Service.

Note This field is ignored if the **Save shared configuration to DB on IM configuration updates** option is checked (in other words, it is ignored for the primary Connector Web Service).

n. Click **Next**. The following screen appears.



o. Enter the server name or IP address of the machine where PSOM Web Service is installed in the **Machine name (or IP address) of the main Web Service** field.

Note PSOM Web Service must be installed before the Connector Web Service installation is performed.

p. Enter the username for connecting to PSOM Web Service in the **User name used to connect to the main Web Service** field. Administrator is the default.

q. Enter the password for connecting to PSOM Web Service in the **Password for the user** field. The default password is provided.

r. Enter the number of seconds the Connector Web Service should wait before reattempting to initialize an Integration Module in the **If initialization fails, attempt to retry again in x seconds** field. If initialization fails, PSOM creates an alert against the application sensor for the failed instance.

s. Enter the number of seconds the Connector Web Service should wait for an Integration Module to complete initialization in the **Timeout for initialization in seconds** field.

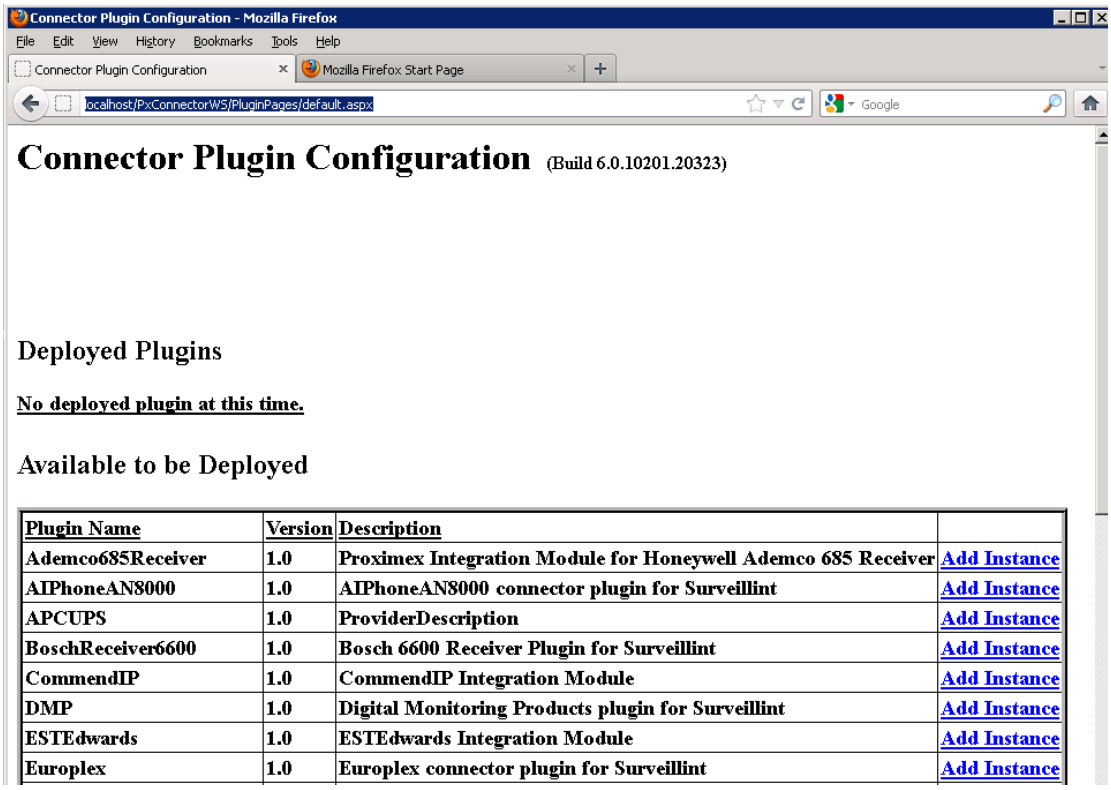
t. Enter the number of seconds that Integration Modules should wait between requests for tracking trail information in the **Tracking object polling interval in seconds** field. This field only pertains to Integration Modules that convey tracking trail information to external 3rd party systems.

u. Click **Finish**. Click **OK** when prompted, then **Close** to complete installation.

Step 2 Test whether the Connector Web Service is installed correctly, open a web browser and navigate to http://localhost/PxConnectorWS/PluginPages/default.aspx. The following window should appear.

Note If you do not see this window, ASP.NET may not be installed or allowed.

You can also access the Connector PlugIn Pages from the Start menu: **Start > All Programs > Cisco Physical Security Operations Manager 6.1 Services > Connector Plugin Page**.



If you receive an "Access is denied" message, then IIS may not be setup correctly to integrate with Windows Authentication mode.

Note The Connector Plugin Configuration page is restricted to access by administrators only. If you attempt to connect this page from a user id that is not in the local Administrators group, your access will be denied. If you are already an Administrator, but you still see the “Access is denied” message, your IIS server may not be properly configured to integrate with Windows Authentication.

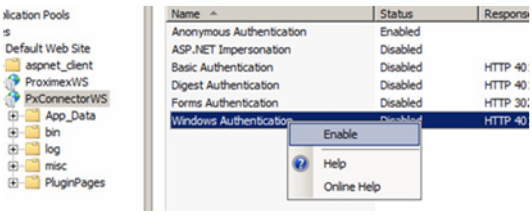
Step 3 Open **Control Panel > Administrative Tools > Internet Information Services**.

Step 4 Expand the hierarchy in the left pane to find PxConnectorWS.

Step 5 Right-click the **PxConnectorWS** icon and select Properties.

Step 6 Click the **Directory Security** tab.

Step 7 Edit the **Anonymous access and authentication control** to turn on **Integrated Windows authentication** for the Authentication Access group.



You can install Integration Modules that enable the Connector Web Service to integrate with access control systems and other external systems. The documentation for all supported Integration Modules is located in the C:\Inetpub\wwwroot\AdministrationConsoleHelp directory.

You must restart the PSOM Services whenever you add or remove an Integration Module instance from a Connector Web Service installation. See *Administering Cisco Physical Security Operations Manager* for instructions.

Installing PSOM Consoles

To install PSOM Consoles, follow these steps:

Procedure

Step 1 Launch the PxConsoleSetup.msi file.

Accept all default settings and proceed through installation. Click **Done** at the end.

This installs the Administration Console, Operation Console, Alert Management Console, Video Management Console, Business Logic Console, and Instant Messenger Console.

Step 2 Verify installation was successful:

a. Select **Start > All Programs > Cisco Physical Security Operations Manager 6.1 > Administration Console**.

The Logon window appears.

b. In the **Server Name** field, enter **localhost**.

c. In the **User Name** field, enter **Administrator**.

d. In the **Password** field, enter **cisco**.

e. Click **Logon**.

If you receive an error message indicating that login failed due to the lack of a Web Service, then follow these steps:

Step 3 Select **Start > Control Panel**, then double-click the **Administrative Tools** icon from the Classic view.

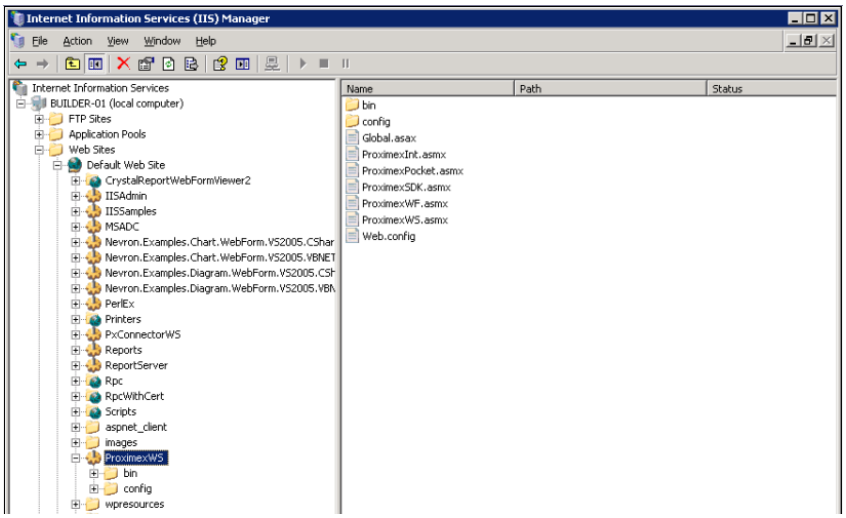
Step 4 Double-click **Services**.

Step 5 Ensure that the following services are started: HTTP SSL, IIS Admin, and Remote Procedure Call (RPC). If one of these services has not been started, select it in the list and click the **Start the service** link.

Step 6 Exit the Services window.

Step 7 In the Administrative Tools window, double click the **Internet Information Services** icon.

Step 8 Locate and right-click **ProximexWS** and select **Properties** from the menu.



The ProximexWS Properties window appears.

Step 9 Click the **Directory Security** tab.

Step 10 Click the **Edit** button in the Authentication and access control area.

Step 11 In the Authentication Methods dialog, select the **Enable Anonymous Access** option.

Step 12 Click **OK** and **OK** again.

Step 13 Exit the Internet Information Services window.

Step 14 Re-open the Services window, and restart the World Wide Web Publishing service.

Step 15 Exit the Services window.

You can now try logging in to the Administration Console again.

Installing PSOM User Services

See Chapter 4, “Installing PSOM User Services.”

Changing the Database Password

During installation, the SQL user PROXIMEX_SYS is created and assigned a password. If you would like to use a different SQL user or password, you can use SQL Server Management Studio to change the PROXIMEX_SYS user password to the desired password.

Note The new SQL user must be db_owner of the ProximexDB database.

To change the SQL user or password for PSOM, follow these steps:

Procedure

Step 1 Select **All Programs > Cisco Physical Security Operations Manager 6.1 Services > Web Service Configuration** from the Start menu.

Step 2 Enter the username for accessing the PSOM Repository in the **Name of Windows User** field.

Step 3 Enter the password for accessing the PSOM Repository in the **Enter the Password** field.

Step 4 Click **Next**.

Step 5 Click **Finish** and **Close**.

Configuring Video Display

If you experience problems when using the Operation Console to take a snapshot of live or recorded video (for example, you get a pink rectangle instead of a snapshot), your video graphics adapter driver may need to be modified. You may need to try disabling DirectDraw and Direct3D hardware Accelerations and see if that makes a difference in taking snapshots with PSOM.

To reduce the hardware acceleration, follow these steps:

Procedure

Step 1 Click **Start** and select **Control Panel**.

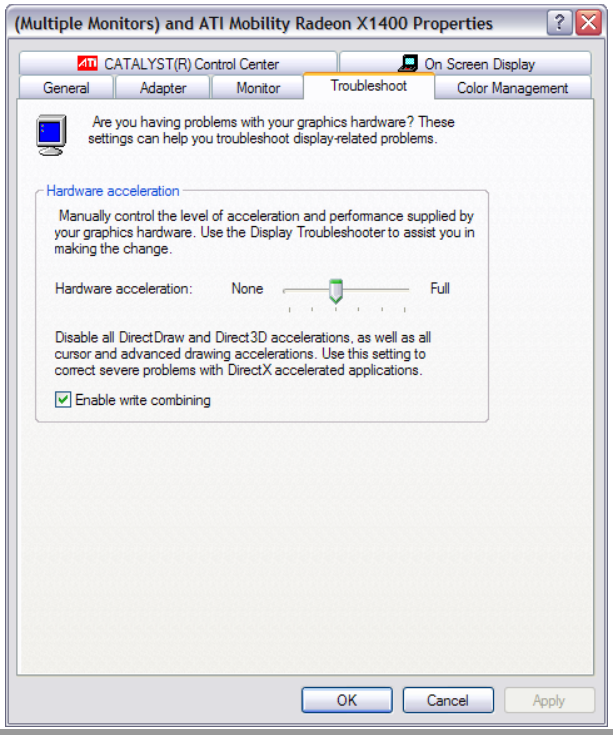
Step 2 Click **Appearance and Themes**.

Step 3 Click **Display**.

Note If you use Windows Classic themes, use the following step, click **Start**, click **Control Panel**, and then click **Display**.

Step 4 On the **Settings** tab, click **Advanced**.

Step 5 On the **Troubleshoot** tab, move the Hardware acceleration slider control to the second position from the left, and then click **OK**.



Logging On or Off

You can log off PSOM Administration Console, and then log back on as a different user, without exiting the Administration Console.

To log off the Administration Console, follow these steps:

Procedure

Step 1 Select **File > Logoff**.

A confirmation dialog appears.

Step 2 Click **Yes**.

To log back on to the Administration Console, follow these steps:

Procedure

Step 1 Select **File > Logon**.

The Logon window appears.

Step 2 Select your login account from the **User Name** field.

Step 3 Enter the corresponding password from the **Password** field.

Step 4 Click **Logon**.

Viewing and Updating Your License Key

Your PSOM license key controls access to the Administration Console, Operation Console, EZ-Track functionality, and other key features. Your license key may have an expiration date depending upon the product purchased.

The license key is a 25-character string.

To view your license key, follow these steps:

Procedure

Step 1 Click **Others** in the Navigation pane.

Step 2 Click **License Manager** in the Navigation pane.

The PSOM License Manager appears.

If you have exceeded your license requirement for an item, it appears highlighted in the list.

To update your license key, follow these steps:

Procedure

Step 1 Click **Others** and then **License Manager** in the Navigation pane.

Step 2 Click the **Update Key** button.

The PSOM License Key window appears.

Step 3 Type your license key in the fields provided and click **OK**.

Integrating Microsoft Bing Maps

If you plan to use Microsoft Bing Maps in your PSOM deployment, you must install the MS Bing Map GIS Plugin on any system where an Operation Console needs to display Bing maps.

You must first install PSOM Consoles, and ensure an active Internet connection to Microsoft Bing Map Web Service, before continuing with these instructions.

Procedure

Step 1 Install the MS Bing Map GIS Plugin by double-clicking the PxGISPluginSetup-MSBing.msi file in the GISPluginInstallers folder.

Step 2 Launch the PSOM Administration Console.

Step 3 Click **Environment** and then **GIS / Map Integration**.

The GIS/map Service Integration Module Configuration window appears.

Step 4 Select **MS Bing Map** and click **Configure**.

The Bing Map Server Configuration window appears.

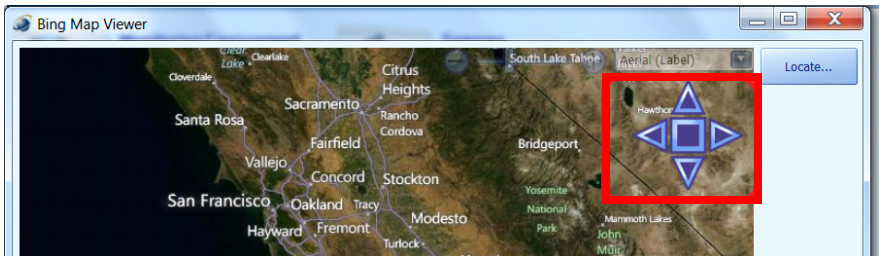
Step 5 If you want to use your own Microsoft Bing Map account, check the **Use Bing Map Key** option and enter the key into the space provided.

Note If the key is invalid, and "Invalid Credentials" appears overlaid on the map when you click **Configure**:

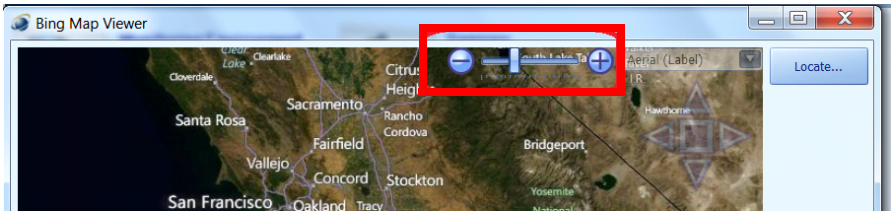
Step 6 Click **Configure** to set the default view presented to users when configuring individual zone/area maps. The default parameters include: Zoom Level, Center Location, and Map mode (Aerial or Aerial/Road).

There are several ways to pinpoint the desired scope and location for the desired map view using the Bing Map Viewer that appears when you click **Configure**:

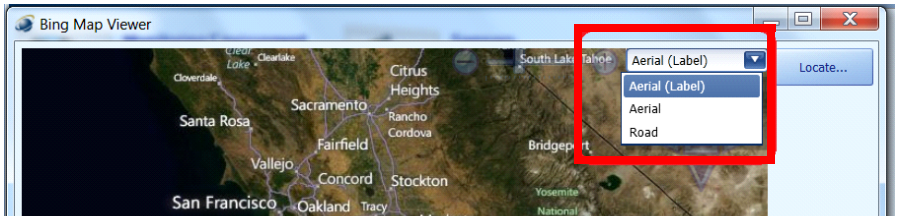
- On-Screen Navigation Controls—These controls appear when the mouse hovers in the right-upper corner of the map. Use the controls to move left, up, right, and down. Center button resets to the default view location and zoom level according to previous configuration.



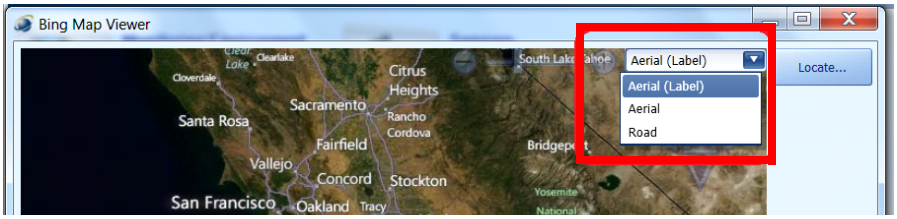
- Zoom Controls—These controls appear when the mouse hovers at the top of the map: Zoom in, out. The mouse wheel can also be used to zoom in and out.



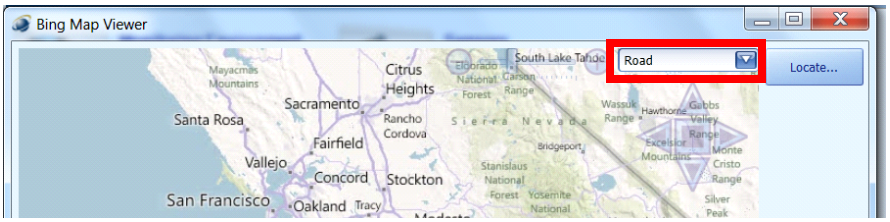
- Map Style Controls—Use this control to switch to a different mode for map style: Aerial (with label), Aerial, Road.



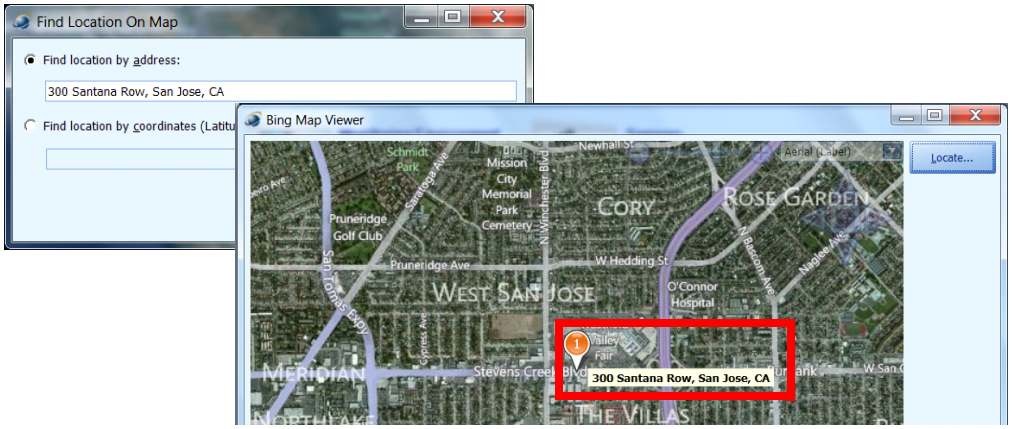
- Map Style Controls—Use this control to switch to a different mode for map style: Aerial (with label), Aerial, Road.



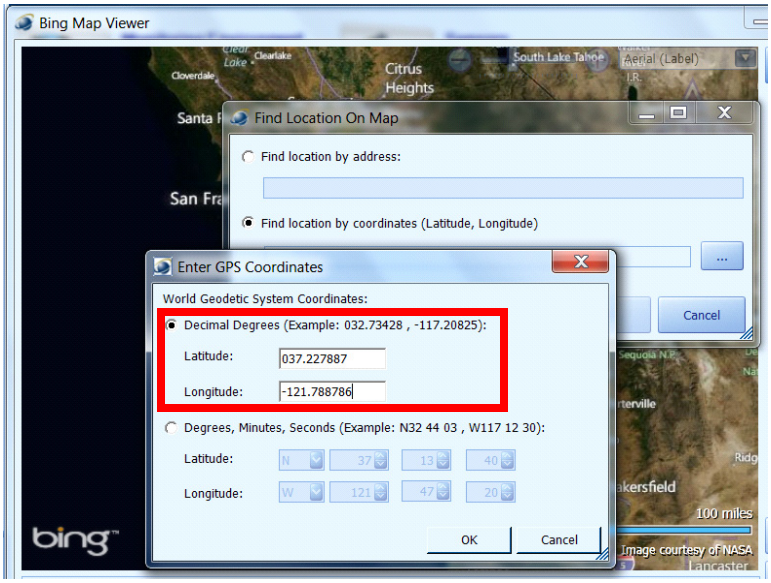
For example, switch to Road style.



- Geocode Tools—Click **Locate** to use Bing to find the desired location:
  - Select **Find location by address**, enter the street address, and click **OK**. Bing displays the location at the center of the map with a temporary push pin button.



  - Select **Find location by coordinates**, enter the latitude and longitude, and click **OK**. Bing displays the location at the center of the map with a temporary push pin button.



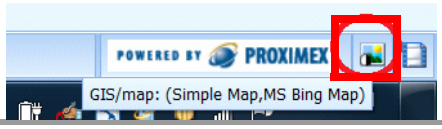
Step 7 Click **OK** to complete configuration.

The Bing Map Server Configuration window reappears.

Select **MS Bing Map** in the list and click **Enable**.

Restart the Administration Console before proceeding with the steps outlined in the "Configuring Microsoft Bing Maps" in *Administering Cisco Physical Security Operations Manager.*

After restarting the Administration Console, verify that Bing Map GIS has been successfully enabled by hovering the mouse over the lower right corner of the window.



CHAPTER 4

Installing PSOM User Services

If you are leveraging PSOM Business Logic, you will want to install the PSOM User Services for enabling PSOM reporting capabilities, controlling camera behavior, or taking action based on video alarms.

This chapter includes these topics:

Overview

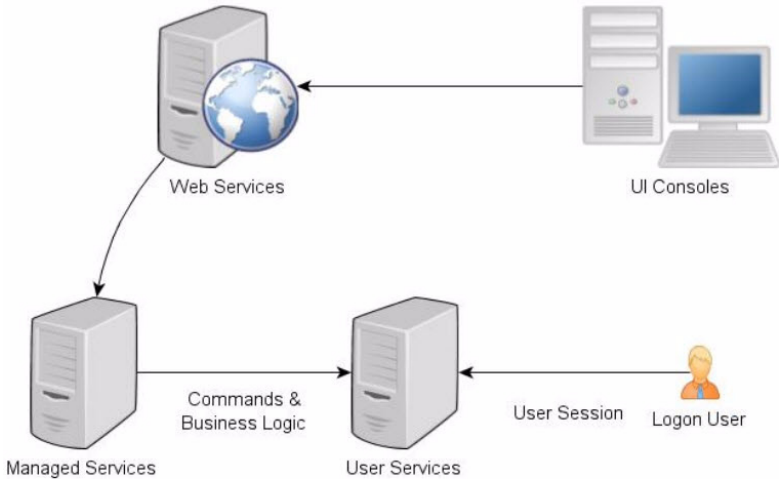
PSOM User Services are an optional set of services for running reports on data collected by PSOM, and controlling video management systems and cameras. PSOM User Services are built as Windows User Sessions applications that expose service endpoints to PSOM Services for a variety of purposes.

PSOM User Services include:

- Reporting Services—Enable PSOM reporting capabilities to be exposed as service endpoints, which can then be consumed and driven by PSOM Business Logic to perform report creation according to predetermined business policies.
- Camera Control Services—Expose camera control commands as service endpoints, which can then be consumed and driven by PSOM Business Logic to control camera behavior (for example, start or stop recording).
- Video Alert Services—Expose video alarms from video vendor subsystems as service endpoints, which can then be consumed and driven by PSOM Event Business Logic to take certain actions when video alarms are raised.

PSOM User Services require that an interactive user is logged onto the server machine at all times. As a Windows User Session application, PSOM User Services must maintain service endpoints to PSOM Services for service automation.

Figure 4-1 Typical Topology of User Services

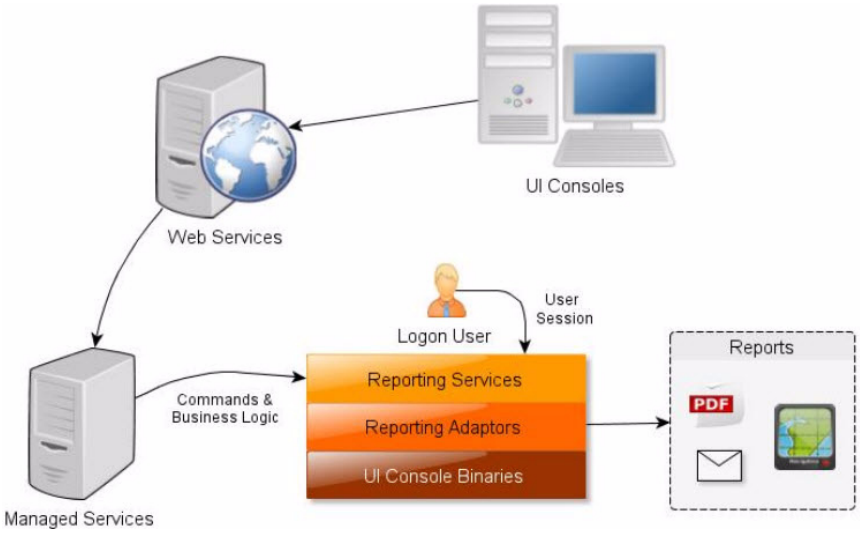


Reporting Services

PSOM Reporting Services expose reporting capabilities as service endpoints, including:

- Generation of Alert Details reports
- Generation of DataSet reports (for tabular or relational data)
- Creation of Alert Mini Maps

Figure 4-2 Reporting Services



Reporting Services also enable reports to be emailed automatically as attachments once report generation is complete.

You can configure Reporting Services from the **Reporting Services** tab of the User Services Configuration. See the "Installing PSOM User Services" section on page 4-5 for configuration instructions or see the "Reconfiguring settings for PSOM User Services" section in *Administering Cisco Physical Security Operations Manager*.

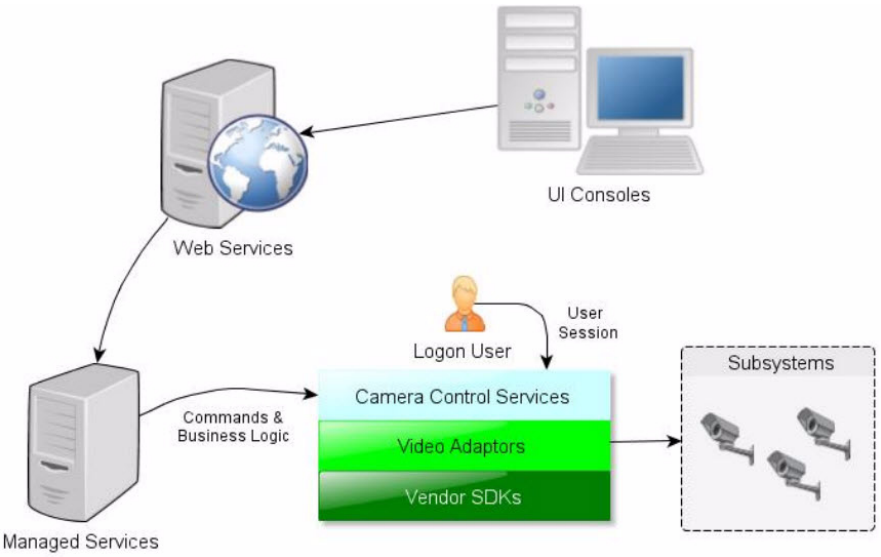
Camera Control Services

Camera Control Services expose commands for controlling camera behavior as service endpoints, including:

- Start or Stop camera recording
- Auxiliary camera control
- PTZ camera movement to preset positions via sensor views

These commands are typically implemented by existing PSOM Video Service Modules for individual video vendors.

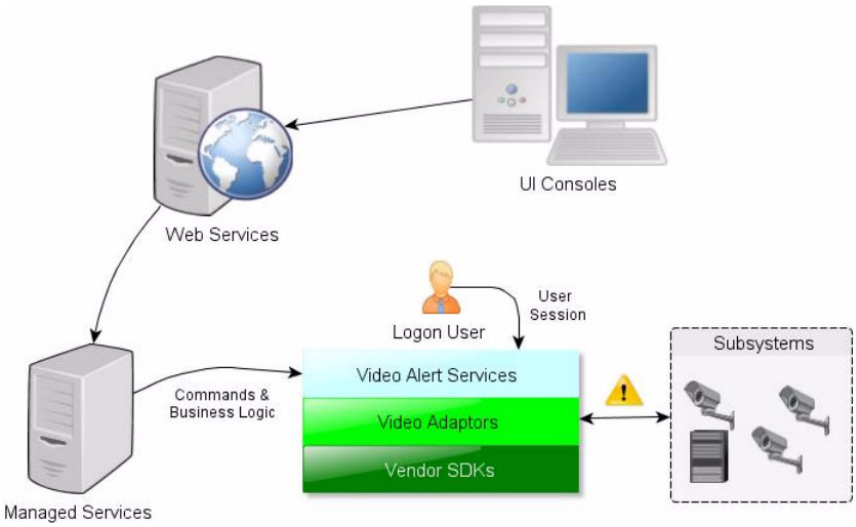
Figure 4-3 Camera Control Services



Video Alert Services

Video Alert Services expose video alarms from video vendor subsystems as service endpoints. Video Alert Service endpoints are leveraged from Event Business Logic running inside Monitoring Logic Services. Only certain PSOM Video Service Modules for individual video vendors support Video Alert Services; see the documentation for the individual Video Service Module.

Figure 4-4 Video Alert Services



Prerequisites

Verify that the following software is installed and running on your machine before you install PSOM User Services:

- PSOM Consoles (on this machine)—PSOM User Services leverage functionality in the PSOM Consoles to implement features, and therefore the PSOM Consoles must be installed before installing PSOM User Services. See the "Installing PSOM Consoles" section on page 3-23.
- PSOM Repository (on this machine or a different machine in the network)—See the "Installing PSOM Repository" section on page 3-2.

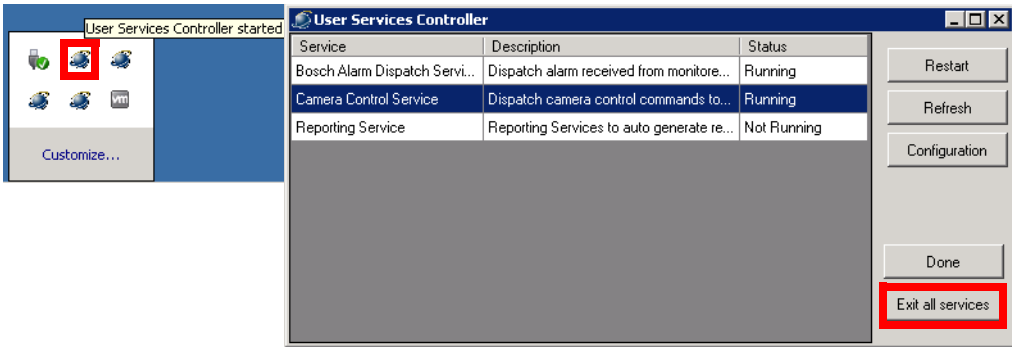
PSOM Web Service (on this machine or a different machine in the network)— See the "Installing PSOM Web Service" section on page 3-4.

Note It is recommended that you create a dedicated Windows or Active Directory Domain account to run the installation of PSOM User Services instead of using the Local System account.

Upgrading PSOM User Services

Procedure

Step 1 Stop the Camera Control Service. Double-click the **User Services Controller** icon in the Windows tray, and click **Exit All Services** in the User Services Controller window.



Step 2 Uninstall the existing PSOM User Services.

Step 3 Install the PSOM User Services by double-clicking **PxUserServiceHostSetup.msi**.

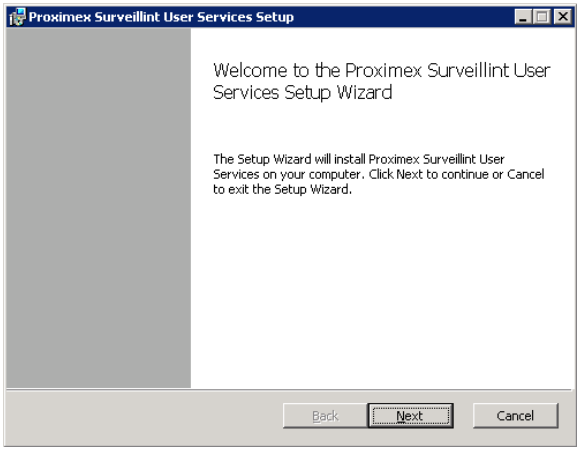
Step 4 Restart PSOM Managed Services.

Installing PSOM User Services

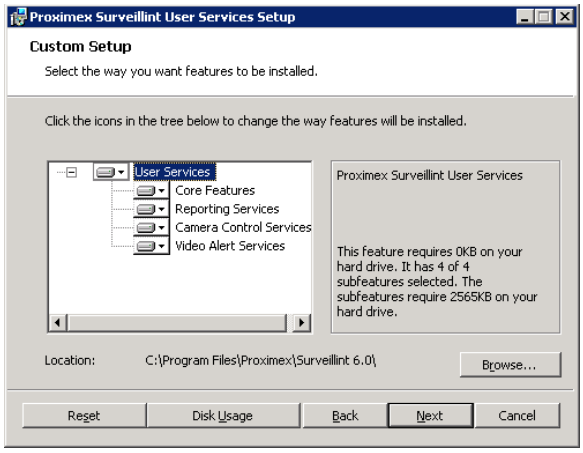
Procedure

Step 1 Install PSOM 6.1.

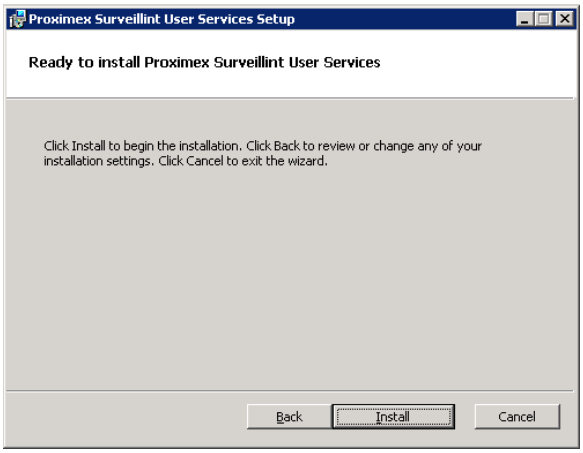
Step 2 Double-click the **PxUserServiceHostSetup.msi** file.



Step 3 Click **Next**. Accept the license agreement and click **Next** again.



Step 4 On the Custom Setup window, leave the component selection and location set to the default values and click **Next**.



Step 5 Click **Install**.

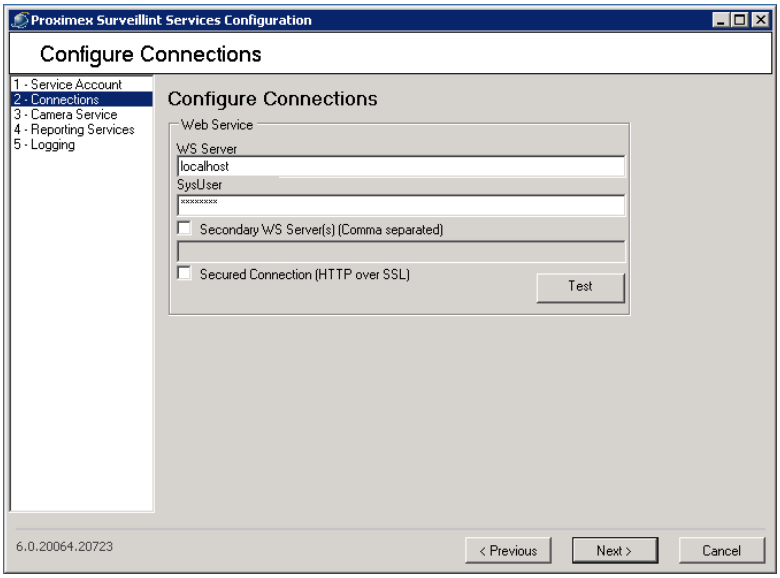
When installation completes, the Services Configuration window appears with Configure Service Account selected.

Step 6 If you decide to use a dedicated Windows account to automatically launch PSOM User Services when the system starts, check the **Use the following local service account for user services and auto logon upon system reboots** option. Enter a valid user name and password in the fields provided. When the system reboots, PSOM User Services will automatically login to the specified service account and lock the system to prevent unauthorized access.

Note By default the user account is PXUSERSERVICEUSER and the password is Pa$$w0rd123.

If the user account you provide does not exist, a new local account will automatically be created.

Step 7 Click **Next** or **2 – Connections**.



Step 8 The **WS Server** field contains localhost unless you installed PSOM Web Service on a different machine in the network. In this case, enter the IP address or server name of the machine where you installed PSOM Web Service.

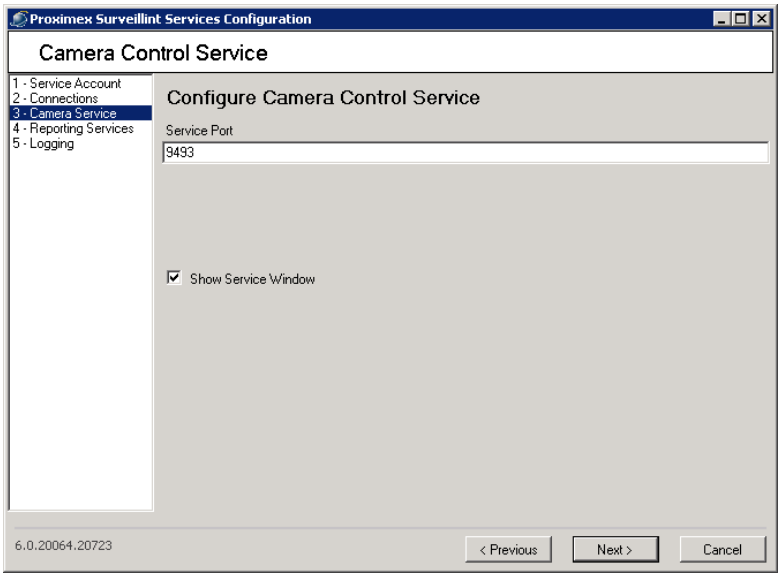
Step 9 The **SysUser** field contains the system user password for the machine where the PSOM Web Service is installed.

Step 10 If you have configured secondary PSOM Web Service instances, list them separated by commas in the **Secondary WS Server** field.

Step 11 If SSL (Secure Sockets Layer) is enabled for Web Services, check the **Secured Connection** option to make sure the User Services use SSL (HTTP over SSL) to connect to the PSOM Web Service. This setting applies to all configured PSOM Web Services.

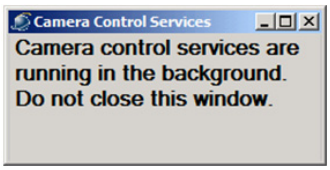
Click **Test Connection** to verify settings.

Step 12 Click **Next** or select **3 - Camera Service** on the left side of the window.



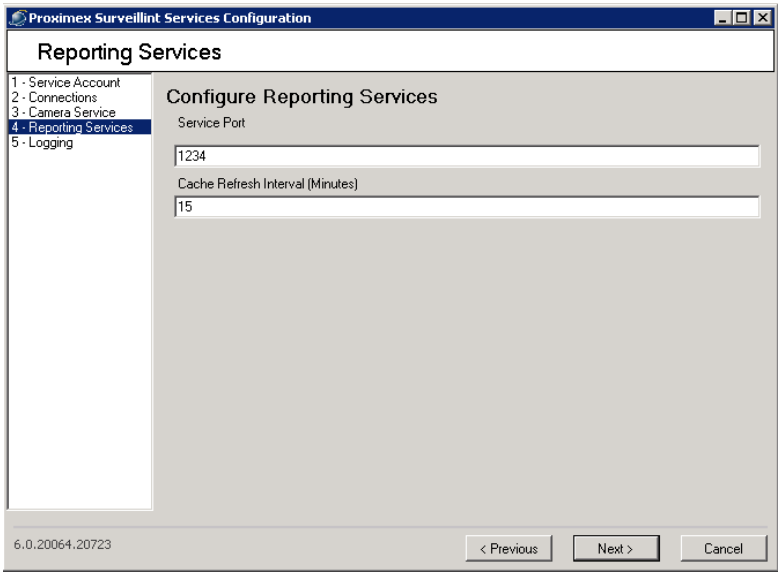
Step 13 The **Service Port** shows the port number under which the Camera Control Service will run by default. Only change this value if you need this service to run under a different port number.

Step 14 Uncheck the **Show Service Window** option if you do not want the Camera Control Service to display the following window while it is running.



Note Do not close the Camera Control Services window while the service is running.

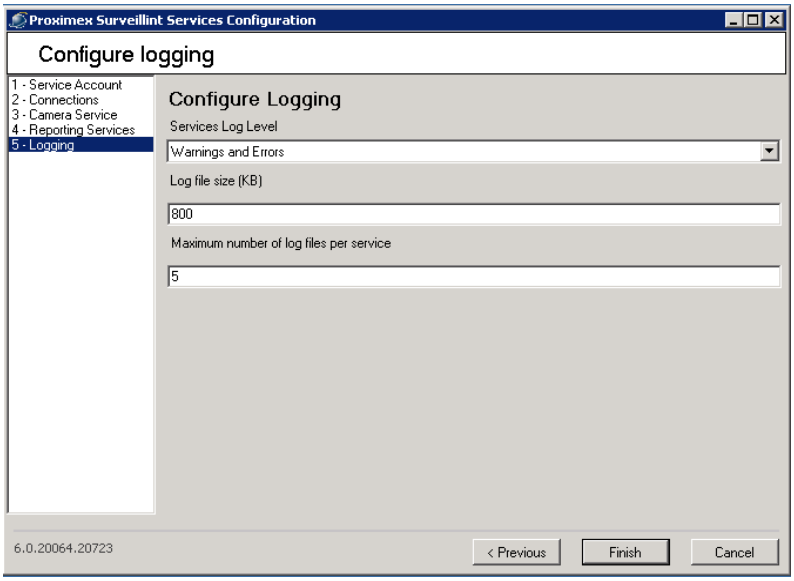
Step 15 Click **Next** or select **4 - Reporting Services** on the left side of the window.



Step 16 The **Service Port** shows the port number under which the Reporting Services will run by default. Only change this value if you need this service to run under a different port number.

Step 17 In the **Cache Refresh Interval (Minutes)** field, enter how often the Reporting Services will refresh its cache of sensor and monitoring hierarchy information. Caching is done to improve performance with regards to reporting.

Step 18 Click **Next** or select **5 - Logging** on the left side of the window.

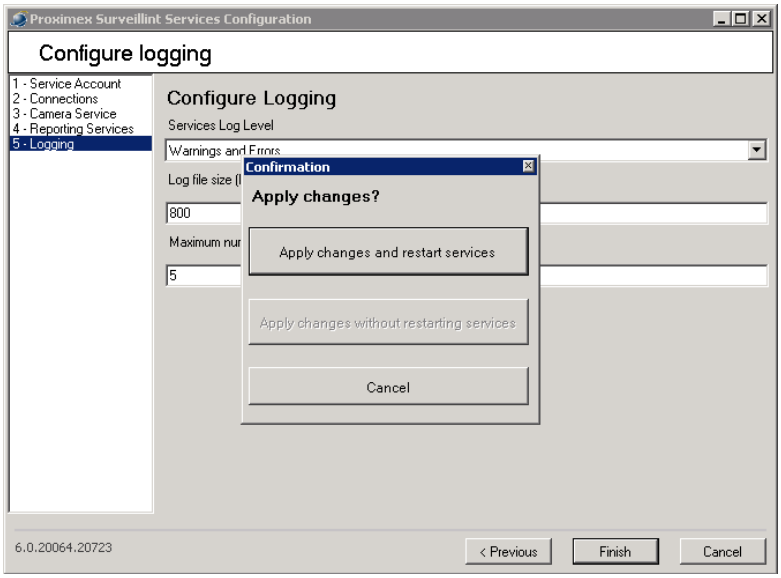


Step 19 From the **Services Log Level** field select the level of messages that should be retained in the log. Choices include: **Everything**, **Informational**, **Warnings and Errors**, and **Errors Only**.

Step 20 In the **Log file size** field, enter the maximum size (in kilobytes) that you want to allow for each log file generated by PSOM Services.

Step 21 In the **Max number of log files per service** field, enter the maximum number of log files that can be generated by each PSOM Service. The default is 5.

Step 22 Click **Finish**.



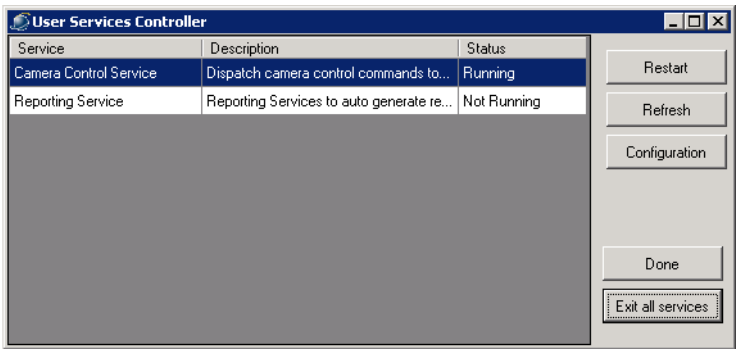
Step 23 At the prompt that appears, click **Apply changes and restart services**.

Step 24 Click **Finish**.

Step 25 To verify successful installation of PSOM User Services, look in the Windows system tray for these icons:

Since user services are running under your current logon user session the services will be automatically stopped once you log off your current session. Only one instance of each user service can run at a time per computer. If multiple users are logged onto the computer, the user services only launch with the first login.

The system tray contains an icon for each PSOM User Service plus an icon for the Service Controller. Double-click the Service Controller icon to open the User Services Controller window.



From this window you can reconfigure or restart PSOM User Services.

Note User Services are designed to launch automatically when a user logs on. Therefore, ensure that only users with Administrative privileges logon to the computer where User Services are running.

To avoid issues, you can enable automatic logon to Windows by opening a Command Prompt and executing this command:

control userpasswords2

In the dialog box the appears, uncheck the **Users must enter a user name and password to use this computer** option.

CHAPTER 5

Deploying Web Access

This chapter describes how to install Web Access for enabling users to access PSOM from web browsers on mobile devices.

This chapter includes these topics:

Overview

Web Access is an alternative to the Operation Console that allows operators remote access to PSOM via a web browser. Web Access offers a subset of the features found in the Operation Console including video playback of both live and recorded video, interactive maps, management of alerts, and inspection of sensors.

Many users can connect to one Web Access server simultaneously, but PSOM isolates each user and shows data tailored to each individual user as configured by security settings in the Administrator Console. This is unlike the Operation Console where software must be installed on each workstation that is to use it.

Like the Operation Console, administration for Web Access is handled via the Administration Console—there is not a web version of the Administration Console.

Note Web Access video support includes these vendors for the 6.0 release: Cisco VMS, Genetec Omnicast, Milestone Corporate.

How Operators Connect to PSOM from a Web Browser

Rather than launching an application installed on a computer, the operator will instead open a web browser and type in a web address (URL) to go to Web Access, similar to accessing any other web site. Internet Explorer 9 (or newer) is recommended for the best experience (with compatibilty mode turned off). Other web browsers might also work, but are not fully supported by PSOM.

Installing Web Access

Web Access must be installed on Internet Information Services 7 (II7) or newer running on Windows Server 2008 R2.

To install Web Access, follow these steps:

Procedure

Step 1 Right-click the **PxWebAccessSetup.bat** file and select **Run as administrator**.

Step 2 In the Welcome window, click **Next**.

Step 3 Accept the license agreement and click **Next**.

Step 4 In the Web Access Setup window, enter the host name for the machine where PSOM Web Service is installed in the **Web Service host name** field. This must be set to localhost for Single Sign On; see the "Configuring Web Access for Single Sign On (SSO)" section on page 5-3.

Step 5 Select the web site where PSOM Web Service is running from the **Install PSOM Web Access to the web site** field; typically **Default Web Site**.

Note In Internet Information Services (IIS), the web server component of Windows Server, there is one or more web sites; by default, there is one named Default Web Site. Each web site can be configured to use a custom host header or binding to produce a URL; see Windows Server documentation.

Step 6 Enter a subdirectory for accessing the Web Access application at the chosen web site in the **Install PSOM PxWebAccess to the application named** field. The default is PxWebAccess.

See the next table to understand how values entered in this screen translate to a complete URL for users to enter in a Web browser.

Host Header	Web Application	URL
www.mycompany.com	PxWebAccess	http://www.mycompany.com/PxWebAccess/
psom.mycompany.com	WebAccess	http://psom.mycompany.com/WebAccess/

Step 7 If you want to use a custom application instead of PxWebAccess, check the **Use a custom app pool instead of PxWebAccess** option and select the application pool to use from the menu.

Note You must leave this option unchecked to enable Single Sign On because Web Access must run under the PxWebAccess local Windows account. See the "Configuring Web Access for Single Sign On (SSO)" section on page 5-3.

Step 8 Click **Next**.

Step 9 In the Destination Folder window, select the location where you want to install the Web Access application on your server and click **Next**.

Step 10 In the Ready to Install window, click **Install**. The software is installed in the chosen directory.

Step 11 When a window appears that informs you that the installation is completed, click **Finish**.

Configuring Web Access for Single Sign On (SSO)

Web Access supports two authentication modes: authentication via PSOM and Single Sign On (SSO) via Windows authentication. With Windows authentication, the user's credentials are collected when they logon to Windows; Internet Explorer passes credentials seamlessly to the web application without re-prompting the user to login.

For more information about ASP.NET security see *How ASP.NET Security Works* at this URL: http://msdn.microsoft.com/en-us/library/ks310b8y.aspx.

To use SSO for Web Access, follow these steps:

Procedure

Step 1 PSOM Web Service must be configured to use Active Directory/Single Sign On (SSO). During configuration of PSOM Web Service, select the **Check to enable Active Directory Client WS authentication** option. See the "Configuring Active Directory for PSOM" *Administering Cisco Physical Security Operations Manager* for complete steps to configuring PSOM for SSO.

Step 2 Verify that you can login to the Operation Console using SSO.

Step 3 Web Access and the PSOM Web Service must be running on the same server machine.

Step 4 When installing and configuring Web Access, set the **Web Service host name** field to localhost. If you have already installed Web Access, you can change the configuration by editing the WebServiceHost parameter in the AppSettings.config file (usually stored in C:\inetpub\wwwroot\PxWebAccess\Configuration):

<add key="WebServiceHost" value="LOCALHOST" />

Step 5 The Web Access application pool must be running under the PxWebAccessUser local Windows account which is created during Web Access installation. If you choose to use a different user account for the Web Access application pool, you need to manually change the web.config file for the PSOM Web Service to specify this account. The account must be in the local Users group.

Step 6 Modify the web.config file for Web Access in a text editor (for example, Microsoft Visual Studio). It is usually located in C:\inetpub\wwwroot\PxWebAccess.

Step 7 Navigate to this code block:

```
<!-- Forms Authentication BEGIN -->
<authentication mode="Forms">
        <forms loginUrl="~/Security/LogOn" timeout="2880" />
</authentication>
<!-- Forms Authentication END -->
<!-- Windows Authentication BEGIN -->
<!--
        <authentication mode="Windows" />
        <identity impersonate="true" />
    -->
<!-- Windows Authentication END -->
```

Step 8 Comment out the Forms Authentication code block and uncomment the Windows Authentication code block. The end result should look like this:

```
<!-- Forms Authentication BEGIN -->
<!--
    <authentication mode="Forms">
        <forms loginUrl="~/Security/LogOn" timeout="2880" />
</authentication>
-->
<!-- Forms Authentication END -->
<!-- Windows Authentication BEGIN -->
        <authentication mode="Windows" />
        <identity impersonate="true" />
<!-- Windows Authentication END -->
```

Step 9 Save the web.config file for Web Access.

Note To revert to forms authentication, reverse the steps.

Troubleshooting SSO

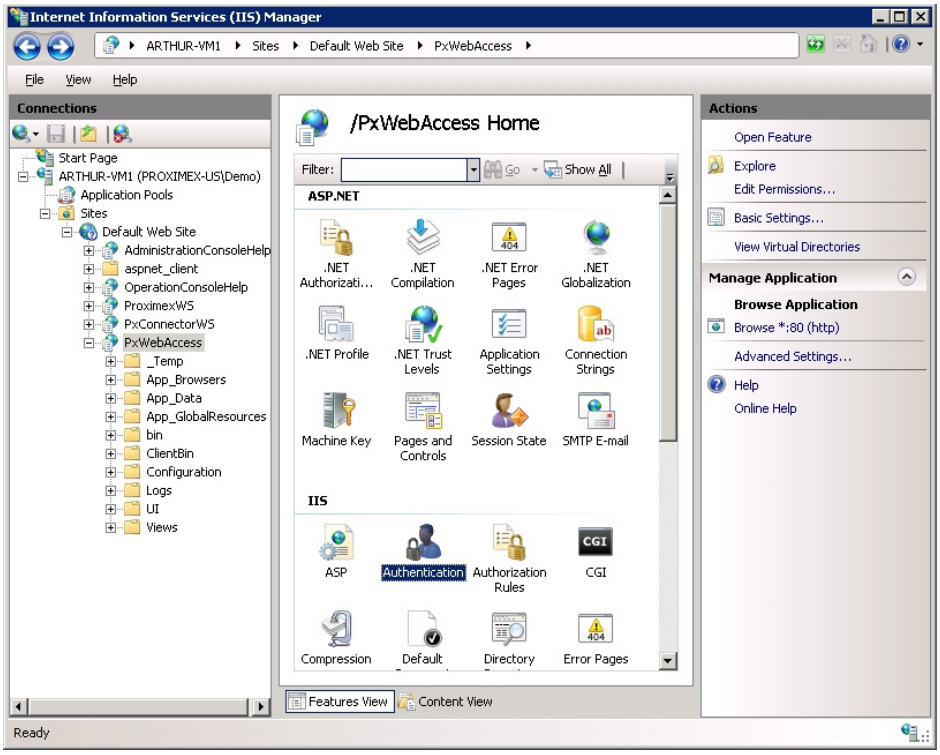
If you receive an HTTP 401.x error with SSO enabled for Web Access, be sure authentication settings for Internet Information Services (IIS) are configured as follows:

- Anonymous Authentication = Disabled
- ASP.NET Impersonation = Enabled
- Windows Authentication = Enabled

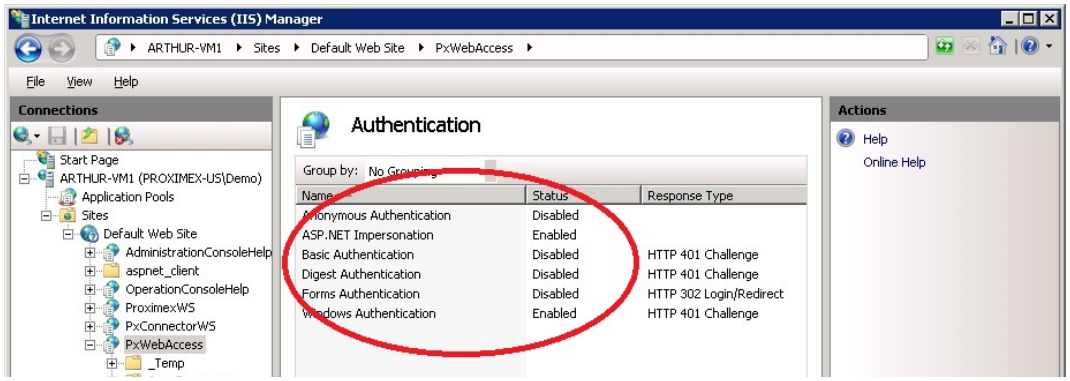
If you receive an event log access message, comment out the following code from the System.Diagnostics.config file.

```
<!--
    <listeners>
        <add name="WebAccessEventLogListener"
        type="System.Diagnostics.EventLogTraceListener"
        initializeData="Surveillint Web Access" />
    </listeners>
-->
```

If you still receive an HTTP error, open Internet Information Services (IIS) Manager, navigate to **PxWebAccess** and click **Authentication**.

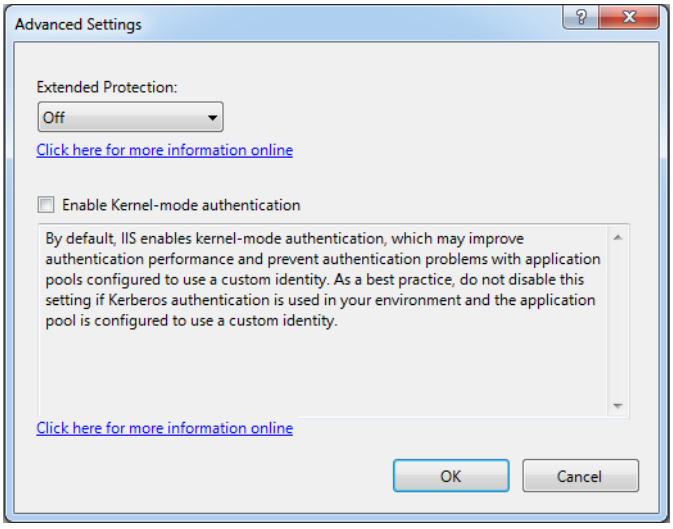


Set the authentication parameters as shown in the following screen.



You might also edit Windows Authentication to change the order in which providers are used so that NTLM is attempted before Negotiate.

Advanced settings can also be configured to disable Kernel-Mode authentication by unchecking the **Enable Kernel-mode authentication** option in the Advanced Settings dialog.


Advanced Settings
Extended Protection:
Off
Click here for more information online
Enable Kernel-mode authentication
By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.
Click here for more information online
OK
Cancel

CHAPTER 6

Enabling SSL Communication for PSOM Web Service

You can enable HTTPS or SSL (Secure Sockets Layer) communication between the PSOM Administration Console, Operation Console and PSOM Web Service. The purpose of such secure, encrypted communication link is to limit exposure for communication eavesdropping in those cases where the Consoles and PSOM Web Service are not in a network secure environment.

This chapter includes these topics:

Prerequisites

- Windows 2008 R2
- PSOM 6.1 installation (not necessarily on the same server):
  - PxDatabaseSetup.msi
  - PxManagedServicesSetup.msi
  - PxConsoleSetup.msi
  - PxWizardPrereq.msi
  - PxWebServiceSetup.msi

Installation instructions for Windows 2008 R2

Procedure

Step 1 Select **Start > Programs > Administrative Tools** and click **Internet Information Services (IIS) Manager**.

Step 2 On the left tree, select **Default Web Site**. And on the right hand pane, click **Bindings…** under Edit Site.

Step 3 In the Site Bindings dialog box that appears, click **Add…**.

Step 4 In the Add Site Binding dialog box, select **https** from the **Type** drop-down list.

Step 5 In the Add Site Binding dialog box, select the SSL certificate the **SSL certificate** drop-down list.

Step 6 In the Add Site Binding dialog box, click **OK**.

Step 7 In the middle area of the Internet Information Services (IIS) Manager window, click **SSL Settings**.

Step 8 Select **Require SSL**, then click **Apply** in the Actions pane at the right of the window.

APPENDIX A

Troubleshooting Problems Uninstalling PSOM Services

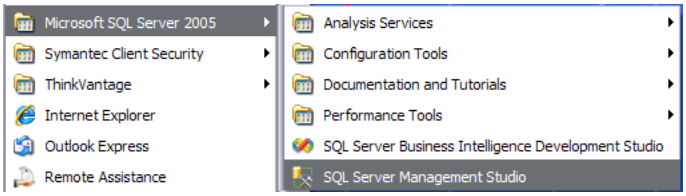
If you receive an error message and cannot uninstall PSOM Services, follow these steps:

Procedure

Step 1 Open C:\Program Files\Cisco PSOM\tempsetup\CreateDb.log. Scroll to the bottom and verify that this error is shown: "ExecuteSqlScriptTask: Error, database does not exist."

You may also see this error: "ExecuteSqlScriptTask: Failed in Executing the SQLScript task: Could not find file "C:\WINDOWS\system32\[TARGETDIR]VelocitySampleSQLJobRemove.sql."

Step 2 Launch SQL Server Management Studio.

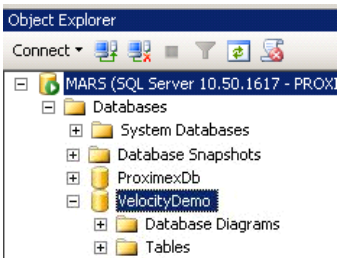


Step 3 Connect to the appropriate instance of the Microsoft SQL Server Database Engine.

Step 4 In Object Explorer, click the server name to expand the server tree.

Step 5 Expand **Databases**, and select the **ProximexDB d**atabase.

Step 6 If you need to run the PSOM demonstration, verify that the VelocityDemo database exists in the same SQL Server instance as the ProximexDB database, as shown next.



a. If the VelocityDemo database does not exist as shown, then create a database called VelocityDemo.

b. Launch Notepad and open the VelocitySampleDbJobsRemove.xml file in the C:\Program Files\Cisco PSOM\tempsetup\ directory.

c. Replace all instances of [TARGETDIR] (including the square brackets) with "C:\Program Files\Cisco PSOM\tempsetup\" (without the quotes).

Step 7 Retry uninstalling PSOM Services.

APPENDIX B

Redundancy and Failover without Clusters

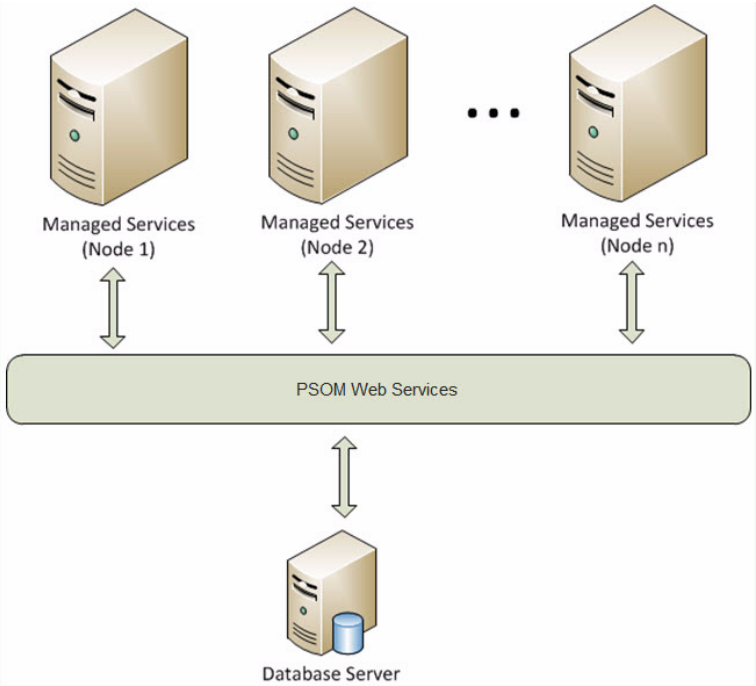
This appendix explains how to configure redundancy and failover for PSOM Managed Services, PSOM Web Service, and PSOM Connector Web Service—without using Microsoft Cluster or NEC Cluster hardware and software configurations. Achieving high availability and failover support without clustering hardware and software requires a high-bandwidth and highly reliable local network LAN that can support a symmetrical network topology between redundant server nodes.

This appendix includes these sections:

Configuring Redundancy for PSOM Managed Services

PSOM Managed Services can be installed on multiple server nodes to achieve redundancy, load balancing, and failover in case of hardware failure on a server node. Components of PSOM Managed Services can be installed multiple server nodes to achieve redundancy and load balancing.

Figure B-1 Redundancy with Managed Services



PSOM Managed Services use *passive redundancy* to achieve redundancy and failover. With passive redundancy, excess capacity is leveraged to reduce the impact of component failures; when a single node fails, other nodes are still operating independently, which means the overall system continues to function. If a number of nodes fail, a decline in overall system performance can be expected with passive redundancy.

Redundant instances of Managed Services are configured as if in standalone mode; no special configuration is required to enable passive redundancy. When Managed Services instances are running, the relevant nodes are active and processing data.

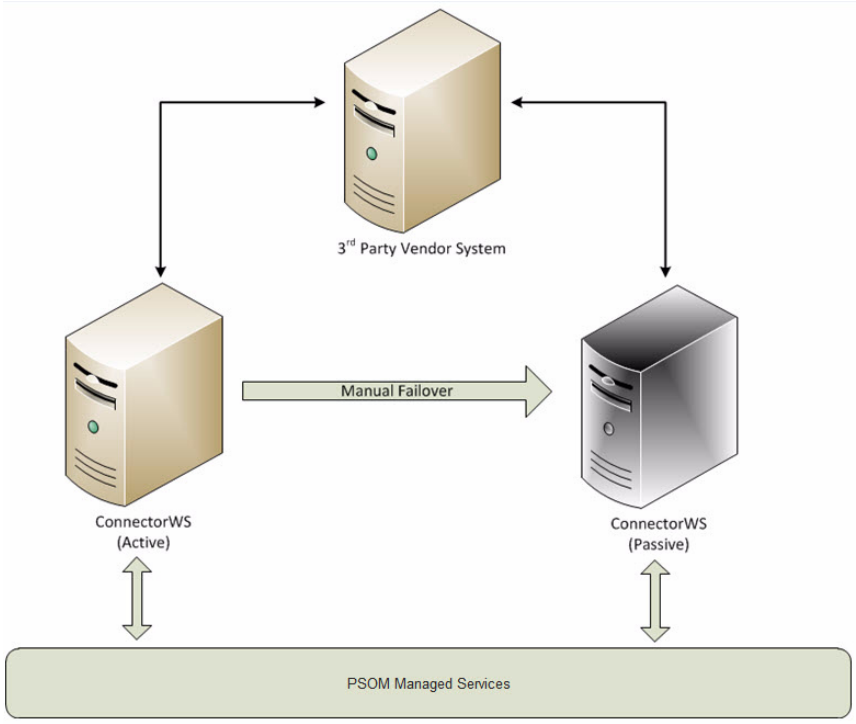
Except for a few temporary queues and read-only performance data that has been cached locally, no state data is stored for individual server nodes running Managed Services; therefore, loss of a node does not result in loss of server state.

Configuring Redundancy for PSOM Connector Web Service

Multiple instances of PSOM Connector Web Service can be installed on multiple server nodes to achieve redundancy and failover in the case of hardware failure. PSOM Connector Web Service uses *active-passive redundancy* to achieve redundancy. Failover to a passive node can be an automated or manual process.

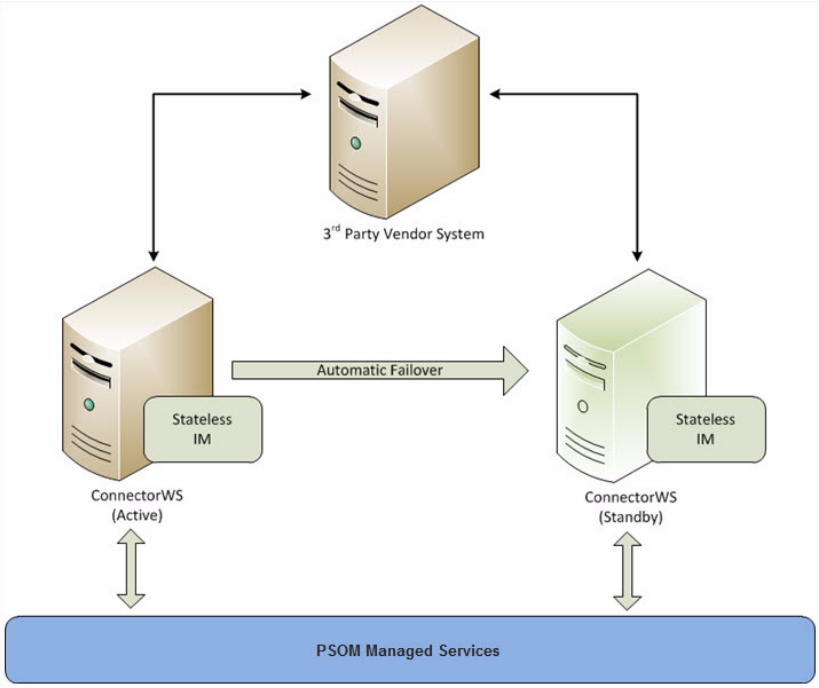
If failover is manual, an administrator must manually trigger failover from the active node to a secondary node via the Managed Services Configuration utility.

Figure B-2 Redundancy with Manual Failover for the Connector Web Service



If failover is automated, PSOM Managed Services will attempt connection to the primary Connector Web Service up to the maximum number of retries, and then failover to a backup Connector Web Service.

Figure B-3 Redundancy with Automated Failover for the Connector Web Service



To enable automated failover for the Connector Web Service, all of the Integration Modules serviced by the Connector Web Service must be stateless and support active standby.

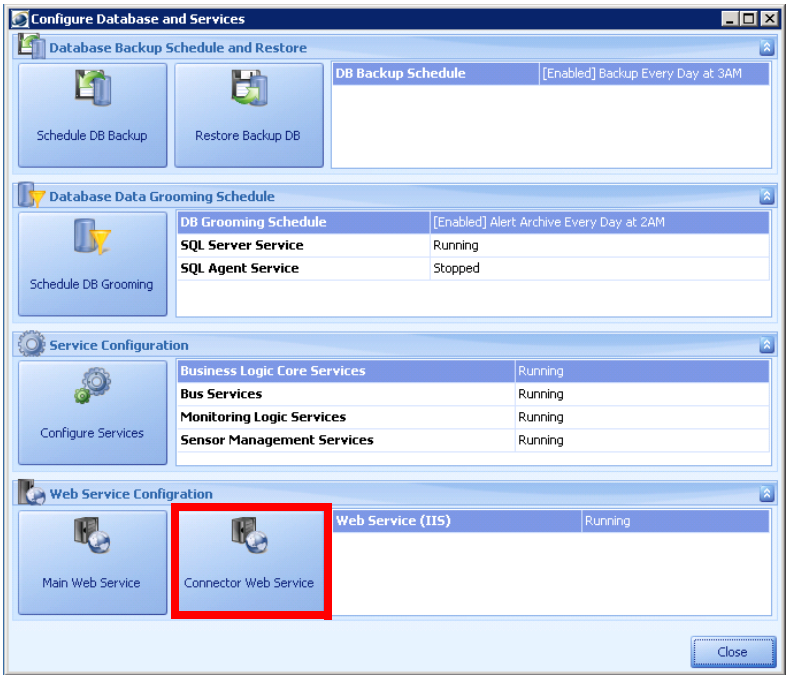
Note Whether manual or automated failover is employed, the primary and backup Connector Web Services must have exactly the same set of Integration Modules installed and configured.

To configure an active/passive pair of Connector Web Services, follow these steps:

Procedure

Step 1 From the PSOM Administration Console, select **Tools** in the Navigation pane, click **Configure DB and Services**, and click **Yes** to log off PSOM temporarily while you configure the services.

Step 2 Click **Connector Web Service**.



The Connector Web Service Configuration window appears.

Step 3 Click **Next**.

The Failover ConnectorWS Configuration screen appears.

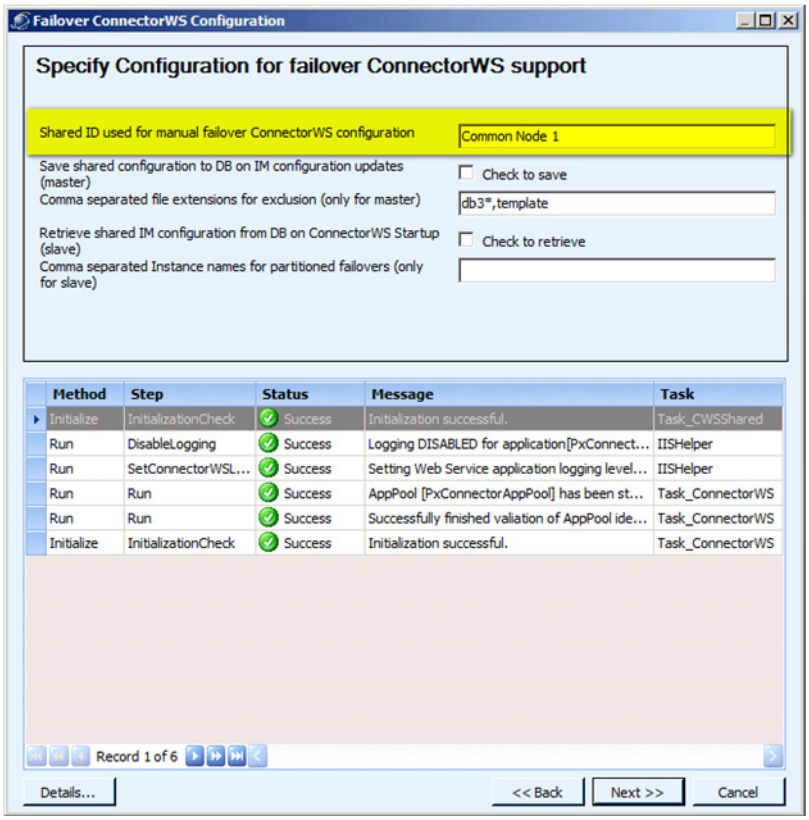
From this screen you can enable a backup Connector Web Service instance to quickly come online with all current Integration Module configurations in the event that the primary Connector Web Service is unavailable.

For example, consider a scenario with these Connector Web Service instances:

- MasterA—INST1 and INST2
- SlaveA_1—INST1
- SlaveA_2—INST2

Under normal circumstances, only MasterA should be running. If MasterA goes down, SlaveA_1 and SlaveA_2 are brought up by external sources to run INST1 and INST2, respectively.

When a Connector Web Service starts (for example, when the Plugin Pages are accessed or a Managed Service is using the Connector Web Service) it initializes itself using the configuration specified on the following screen.



Step 4 Provide a name for the primary Connector Web Service configuration that can be stored in the PSOM Repository and accessed by a failover Connector Web Service in the **Shared ID used for manual failover ConnectorWS configuration** field. The primary Connector Web Service and any backup Connector Web Service instances must all use this same shared ID. If this field is left blank, the configuration will not be stored in the PSOM Repository.

Step 5 If this Configuration Web Service should serve as the primary one, check the **Save shared configuration to DB on IM configuration updates** option. The configuration for this primary Connector Web Service will be saved to the PSOM Repository.

When this option is checked, any changes to files under PxConnectorWS\App_Data (such as configuration of new Integration Modules, removal or updates of Integration Module instances, or any other changes to subdirectories under App_Data) will be saved to the PSOM Repository by PSOM Web Service.

Step 6 If you do not want to backup certain configuration files, enter the file extensions for the files you do not want to backup to the PSOM Repository, separated by commas, in the **Comma separated file extensions for exclusion (only for master)** field.

Step 7 If this Configuration Web Service should serve as a backup one, check the **Retrieve shared IM configuration from DB on ConnectorWS startup** option. The configuration for this Connector Web Service will be retrieved from the PSOM Repository using the Shared ID provided.

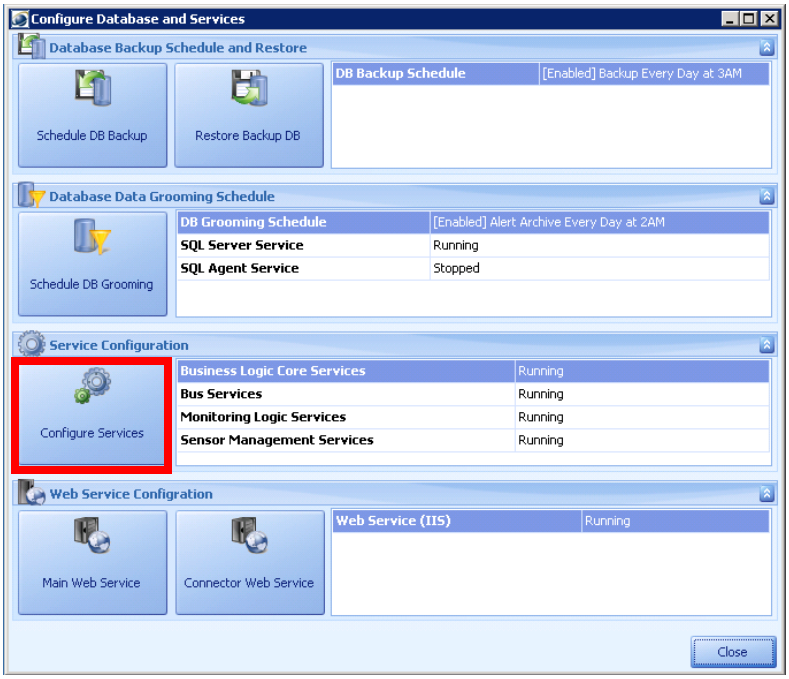
Step 8 If you only want to retrieve certain configuration files (for example for certain Integration Modules), enter the instance names of the Integration Modules you want to retrieve from PSOM Repository, separated by commas, in the **Comma separated Instance names for partitioned failovers** field. Only related files from PxConnectorWS\App_Data will be retrieved from PSOM Repository when the Connector Web Service is restarted.

Leave this field blank to retrieve all configuration information stored for the primary Connector Web Service.

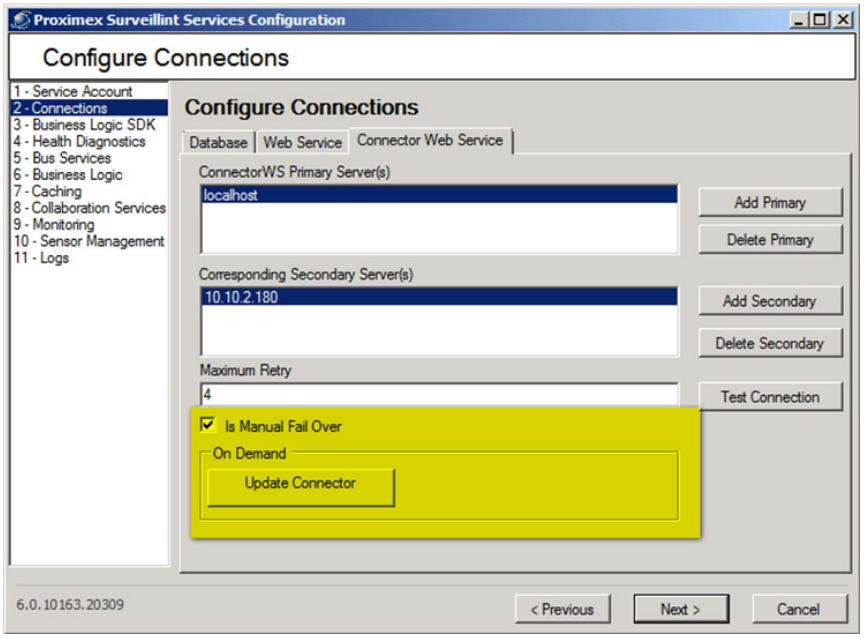
Note This field is ignored if the **Save shared configuration to DB on IM configuration updates option** is checked (in other words, it is ignored for the primary Connector Web Service).

Step 9 Click **Next** and click **Finish**.

Step 10 Back in the Configure Database and Services window, click **Configure Services**.



The PSOM Services Configuration window appears.

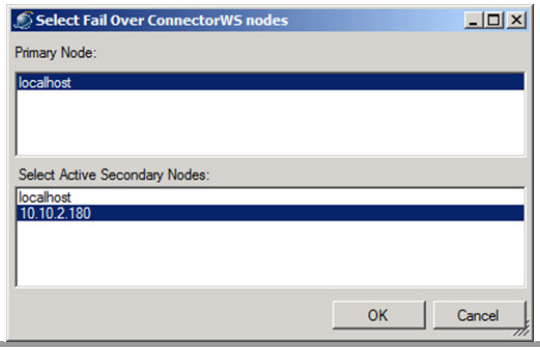


Step 11 Click **2 - Connections** and click the **Connector Web Service** tab.

Step 12 Choose whether to implement automated or manual failover:

- Automated failover—By default, PSOM is configured so that failover to a secondary Connector Web Service is performed manually. For automated failover, the **Is Manual Fail Over** option should not be checked.
- Manual failover—If you want to perform failover manually, check the **Is Manual Fail Over** option.

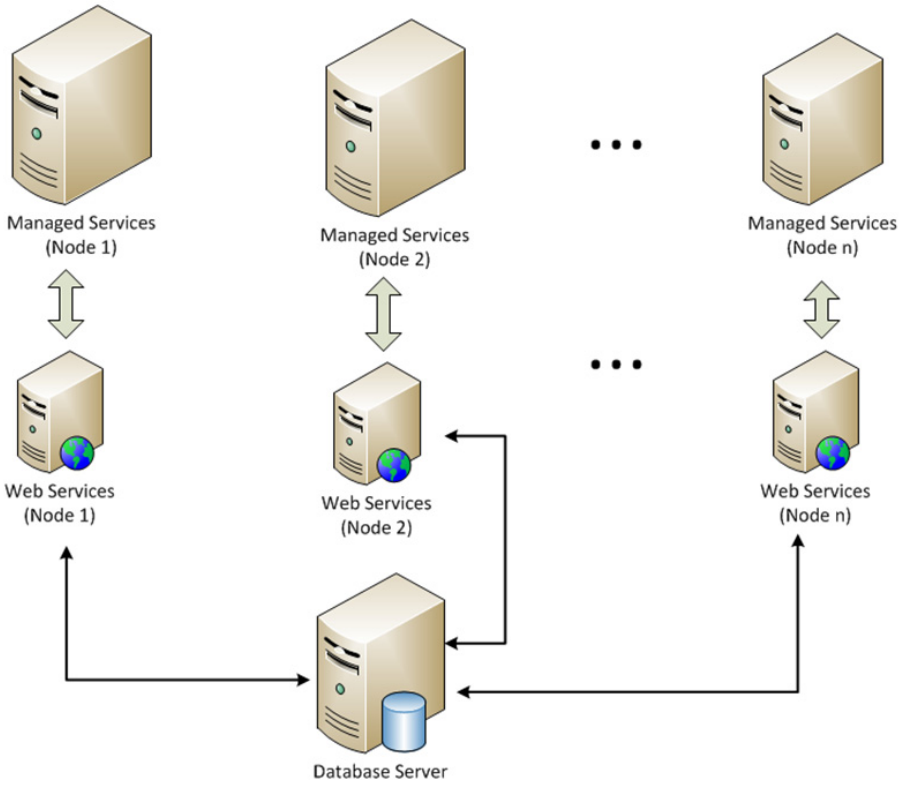
  Then to manually failover the Connector Web Service, click **Update Connector**. In the Select Fail Over ConnectorWS nodes dialog, select the primary node from which to failover, and the secondary node to which to failover. Click **OK**.



Configuring Redundancy for PSOM Web Services

PSOM Web Services are stateless services that serve as an intermediary between PSOM Managed Services and the PSOM Repository (running on the database server). For redundancy and failover, PSOM Web Services can be installed on multiple server nodes.

Figure B-4 Redundancy with PSOM Web Services



PSOM Web Services use *passive redundancy* to achieve redundancy and failover. With passive redundancy, excess capacity is leveraged to reduce the impact of component failures; when a single node fails, other nodes are still operating independently, which means the overall system continues to function. If a number of nodes fail, a decline in overall system performance can be expected with passive redundancy.

Redundant instances of Web Services are configured as if in standalone mode; no special configuration is required to enable passive redundancy. When Web Services instances are running, the relevant nodes are active and processing data.

Except for a few temporary queues and read-only performance data that has been cached locally, no state data is stored for individual server nodes running Web Services; therefore, loss of a node does not result in loss of server state.

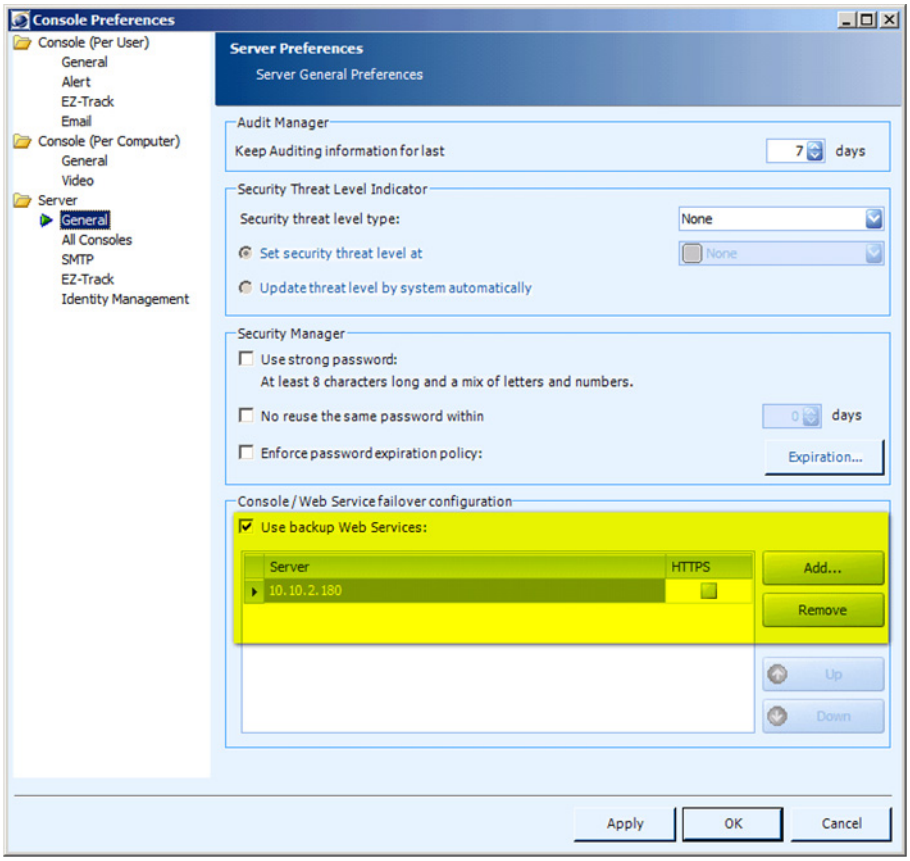
To support high availability, both PSOM Consoles and PSOM Managed Services (and User Services) can be configured with secondary Web Services server nodes.

Note Backup Web Services can be configured for the operational consoles including the Operation Console, Alert Console, Video Console, and Instant Messenger Console. The Administration Console does not support backup Web Services.

To configure backup Web Services for PSOM Consoles, follow these steps:

Procedure

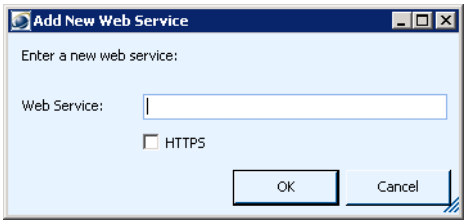
Step 1 Click **Preferences** and **Server > General**.



Step 2 Check the **Use backup Web Services** option.

Step 3 Click **Add**.

The Add New Web Service dialog appears.

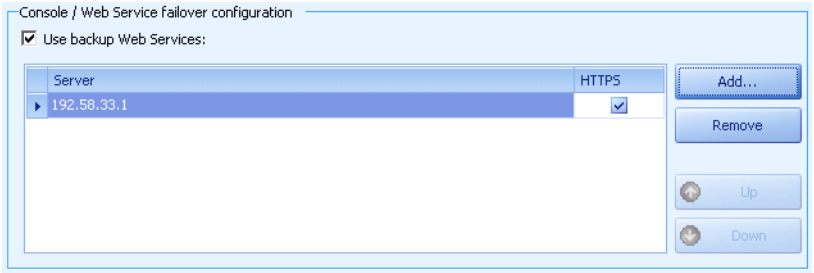


Step 4 Enter the IP address or server name where the backup Web Service is running in the **Web Service** field.

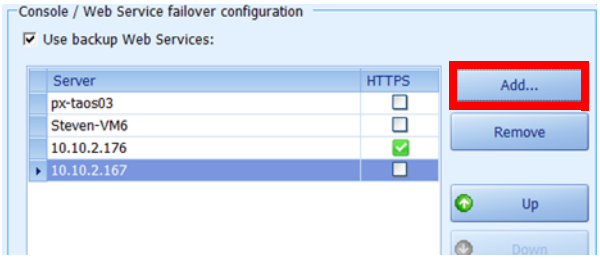
Step 5 Check the **HTTPS** option to use a secure connection for the Web Service.

Step 6 Click **OK**.

The backup Web Service appears in the list.



Step 7 When there are multiple backup Web Services defined, you can rearrange the order of them using the **Up** and **Down** buttons.

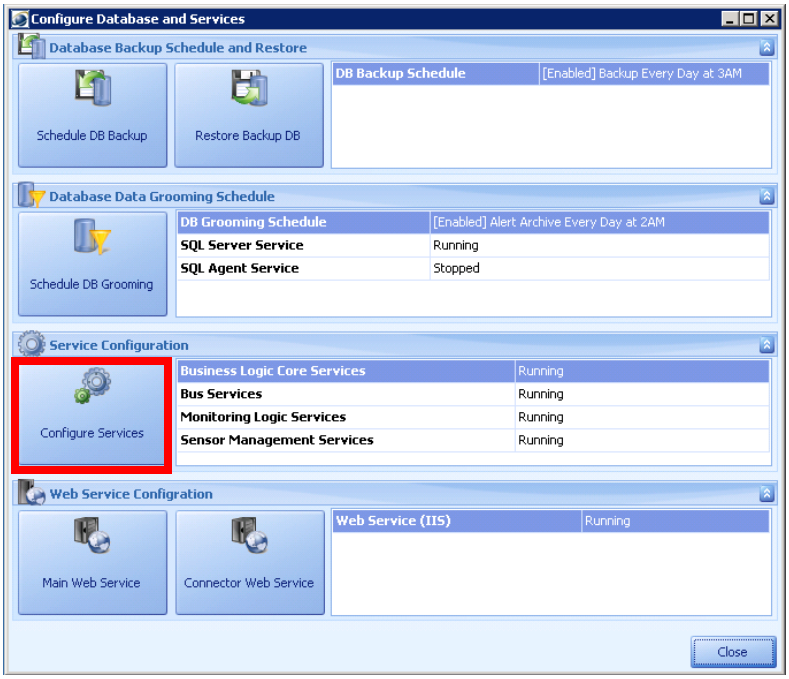


To configure backup Web Services for PSOM Managed Services, follow these steps:

Procedure

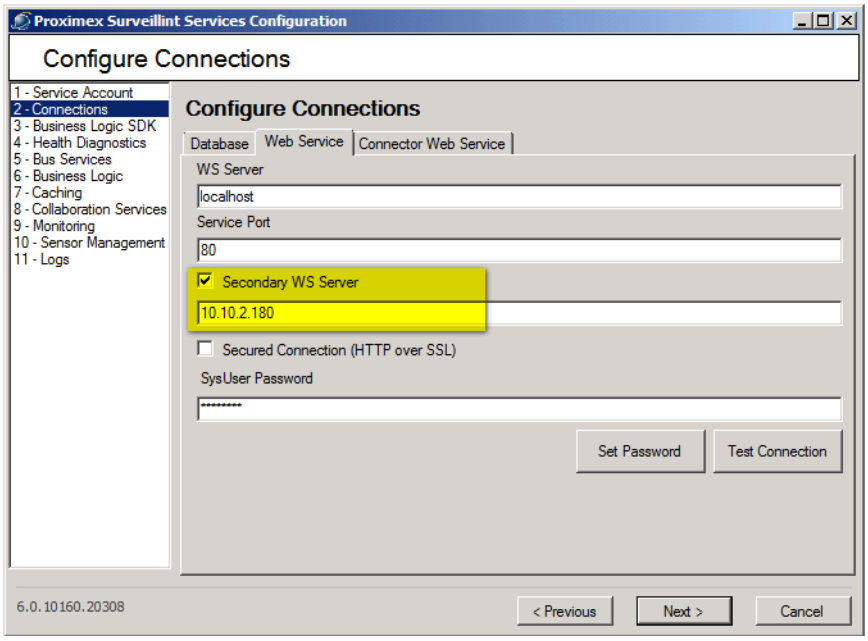
Step 1 From the PSOM Administration Console, select **Tools** in the Navigation pane, click **Configure DB and Services**, and click **Yes** to log off PSOM temporarily while you configure the services.

Step 2 Click **Configure Services**.



The PSOM Services Configuration window appears.

Step 3 Click **2 - Connections** and click the **Web Service** tab.



Step 4 Check the **Secondary WS Server** option and enter the IP address or server name where the backup PSOM Web Service is running.

Step 5 Click **11 - Logs** and click **Finish**. Restart PSOM Managed Services.

Redundancy Scenarios

According to different needs and constraints, you may decide to setup redundancy and failover using one of the following scenarios:

- Multiple sets of single instances (full stack)—While only a small number of server nodes is required to achieve full redundancy on the service tier, the load may not be distributed evenly across nodes.
- Redundant sets of Web Service and Managed Services nodes—Failover is fully automated and load is distributed between redundant nodes, but Connector Web Service becomes a single-point-of-failure (SPOF).
- Redundant Connector Web Services, Web Services, and Managed Services nodes—Failover is fully automated and load is distributed between redundant nodes, but at least 4 nodes are needed to achieve redundancy and the load between redundant Web Services and Connector Web Services is not evenly distributed.
- Full asymmetrical redundancy—This solution offers the greatest flexibility and most comprehensive failover with manual control of Connector Web Service failover. However, it is the most complex configuration and requires at least 6 nodes to implement.

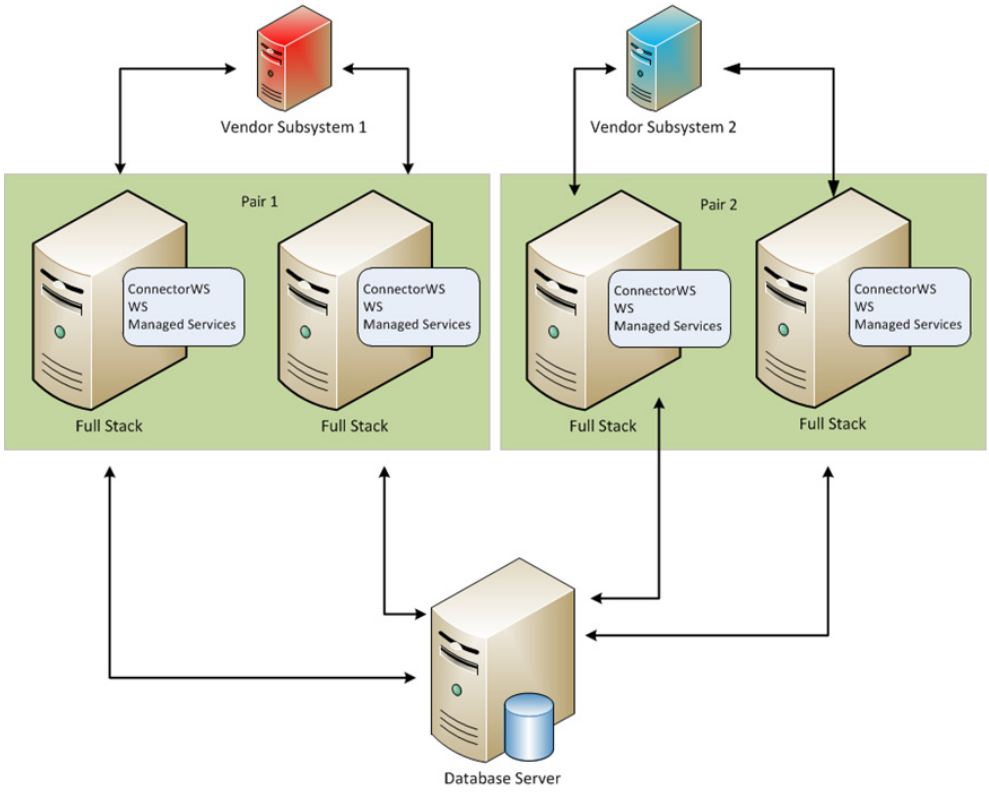
Configuring Multiple Sets of Single Instances (Full Stack)

In this scenario, multiple server nodes within the network are configured with a complete set of PSOM Services: Managed Services, Web Services, and Connector Web Services.

Table B-1 Advantages/Disadvantages of Multiple Sets of Single Instances

Advantages	Disadvantages
Only 2 server nodes are needed to achieve full redundancy.	Load may not be evenly distributed between nodes.
No special configuration is required for the Services. Each service is configured to talk to its local instance.	—

Figure B-5 Full Stack Redundancy Mode



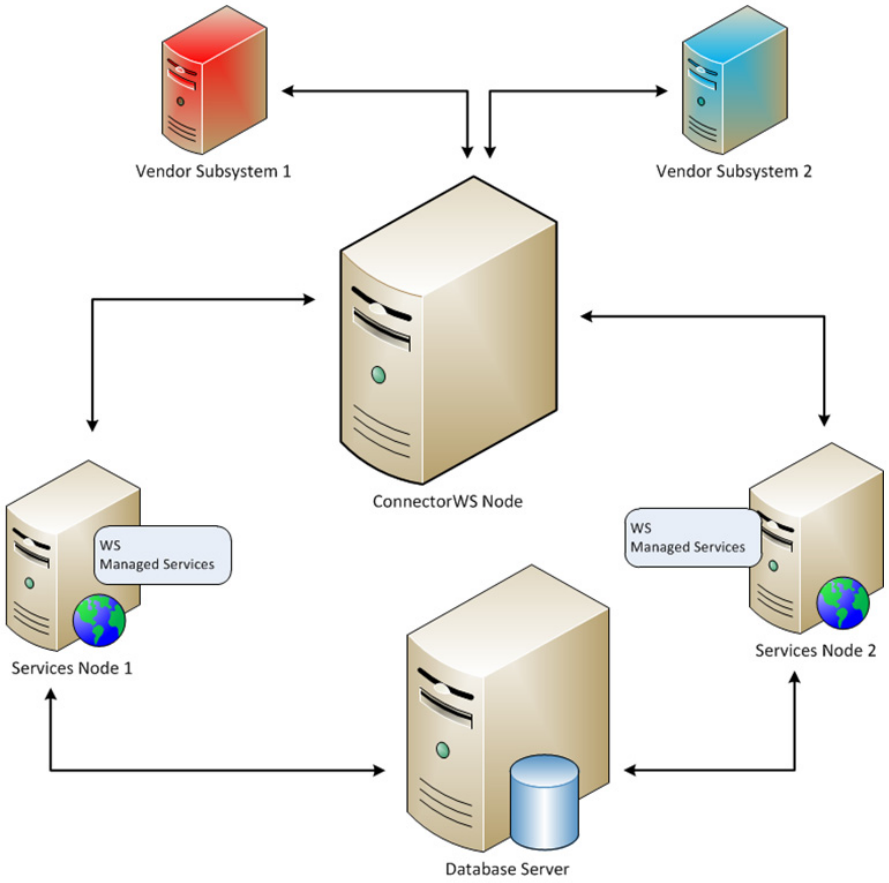
Configuring Redundant Sets of Web Services and Managed Services Nodes

In this scenario, redundant nodes within the network are configured with both the Web Services and Managed Services. The Connector Web Service is not redundant.

Table B-2 Advantages/Disadvantages of Redundant sets of Web Services and Managed Services

Advantages	Disadvantages
Fully automated failover between redundant nodes for Web Services and Managed Services.	Connector Web Service is a single point of failure (SPOF). If this node fails, PSOM cannot receive events from vendor systems, nor send commands to vendor systems.
Load is distributed across redundant nodes for Web Services and Managed Services.	Connector Web Service needs to be configured to use secondary Web Services nodes.
No special configuration is required for the Web Services or Managed Services . Each service is configured to talk to its local instance.	

Figure B-6 Redundant Web Services and Managed Services



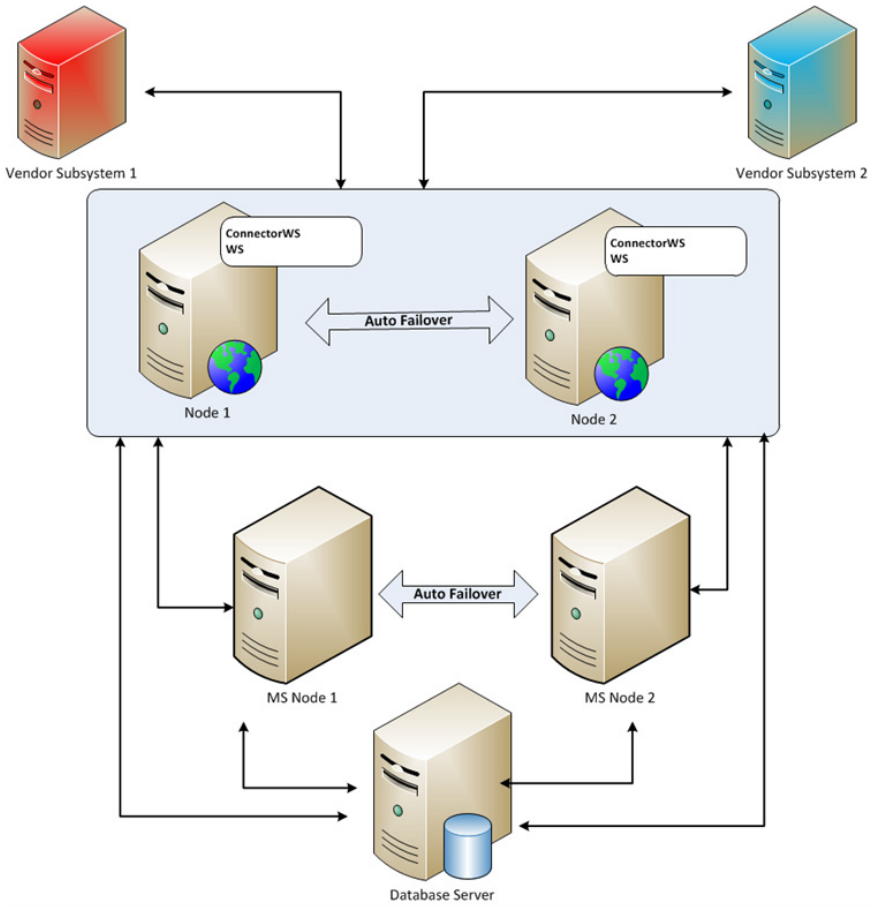
Configuring Redundant Connector Web Services, Web Services, and Managed Services Nodes

In this scenario, multiple redundant nodes within the network are configured with both the Web Services and Managed Services for load balancing and failover. Two redundant nodes are configured with the Connector Web Services.

Table B-3 Advantages/Disadvantages of Redundant sets of Connector Web Services, Web Services, and Managed Services

Advantages	Disadvantages
Fully automated failover between redundant nodes for Connector Web Services, Web Services and Managed Services.	Load between redundant Web Services and Connector Web Services is not balanced across nodes.
Load is distributed across redundant nodes for Managed Services.	Redundant Connector Web Service must have exactly the same installation and configuration as the primary (mirrored) Connector Web Service.
No special configuration is required for the Web Services	Integration Modules instances on the primary and redundant Connector Web Services cannot be in active competition.
—	More nodes are required to achieve redundancy: minimum of 2 nodes for Managed Services minimum of 2 nodes for Connector Web Services and Web Services
—	Connector Web Service must be configured to talk to redundant Web Services nodes. Connector Web Services must be configured with exactly the same sets of Integration Modules (same instance names and descriptions).
—	Managed Services must be configured to talk to redundant Connector Web Services and Web Services. Managed Services must be configured to use automatic failover to Connector Web Services.

Figure B-7 Redundant Connector Web Services, Web Services, and Managed Services nodes



Configuring Full Asymmetrical Redundancy

This scenario is the most flexible, but also most complex. Two redundant Connector Web Services can be deployed with an arbitrary number of Web Services and Managed Services replicated independently on different nodes. For each Connector Web Service instance there must be pairs of nodes (*active-passive*) to achieve redundancy.

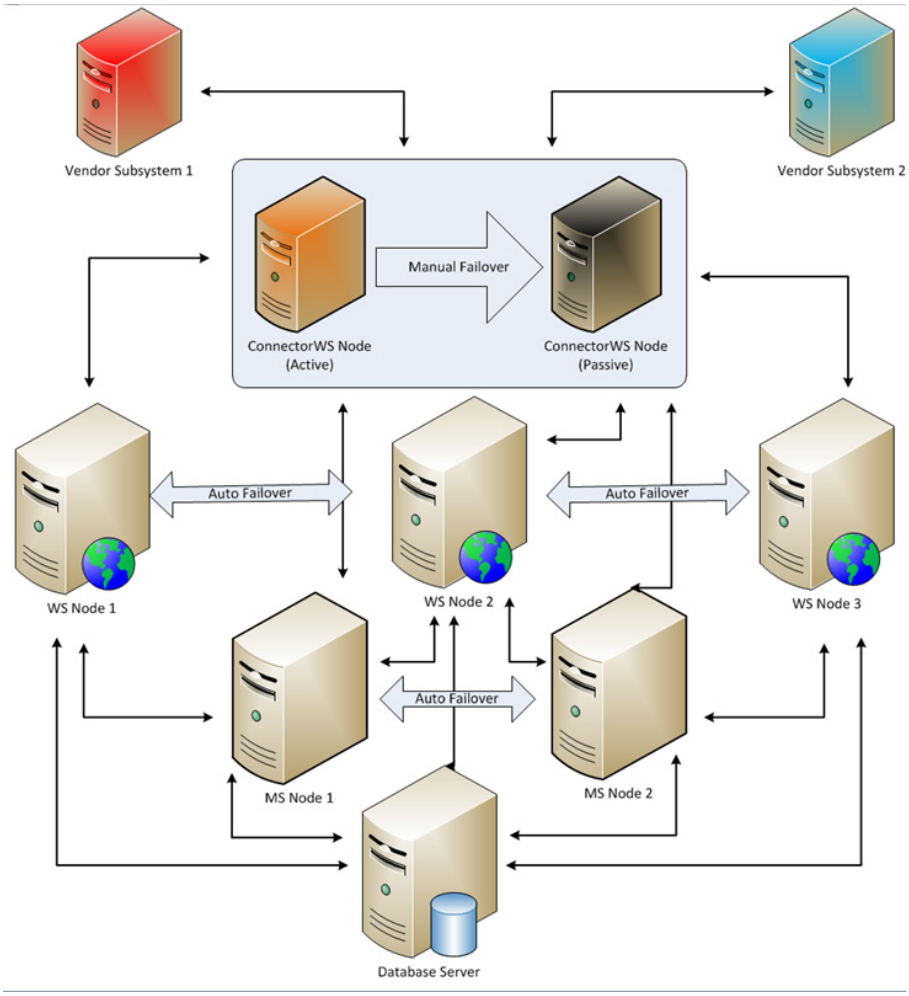
Table B-4 Advantages/Disadvantages of Full Asymmetrical Redundancy

Advantages	Disadvantages
In case of hardware failure, Connector Web Service can failover to a passive node in a managed way.	Connector Web Service failover is still a manual process, but it can be managed by the Managed Services and database.
Fully automated failover between redundant nodes for Web Services and Managed Services.	More nodes are required to achieve redundancy: • Minimum of 2 nodes for Managed Services • Minimum of 2 nodes for Connector Web Services • Minimum of 2 nodes for Web Services

Table B-4 Advantages/Disadvantages of Full Asymmetrical Redundancy

Advantages	Disadvantages
Load is distributed across redundant nodes for Web Services and Managed Services.	Connector Web Service needs to be configured to use secondary Web Services nodes.
No special configuration is required for the Web Services.	Managed Services must be configured to talk to redundant Connector Web Services and Web Services.

Figure B-8 Full Asymmetrical Redundancy



Recommendations and Best Practices

Best practices for implementing failover and redundancy without using Microsoft or NEC cluster are provided in the following table.

Table B-5 Best Practices for Failover and Redundancy

Small Environments	Medium Environments
• Use multiple sets of single instances on two active nodes to achieve redundancy as described in the "Configuring Multiple Sets of Single Instances (Full Stack)" section on page B-12. • Configure Managed Services to talk to the active/primary Connector Web Services node and include the secondary Connector Web Services node as a backup. • Use manual failover for Connector Web Service if the Integration Modules are stateful. Otherwise, use automatic failover for Connector Web Service if the Integration Modules are stateless.	• Use redundant Connector Web Services, Web Services, and Managed Services nodes to achieve redundancy as described in the "Configuring Redundant Connector Web Services, Web Services, and Managed Services Nodes" section on page B-15. • Separate redundancy in Connector Web Services/Web Services nodes and Managed Services nodes. • Set up redundant sets of Web Services and Connector Web Services on two server nodes. • Set up redundant Managed Services on two server nodes. • Use a full mirror between Connector Web Services nodes. • Use manual failover for Connector Web Service if the Integration Modules are stateful. Otherwise, use automatic failover for Connector Web Service if the Integration Modules are stateless.

APPENDIX C

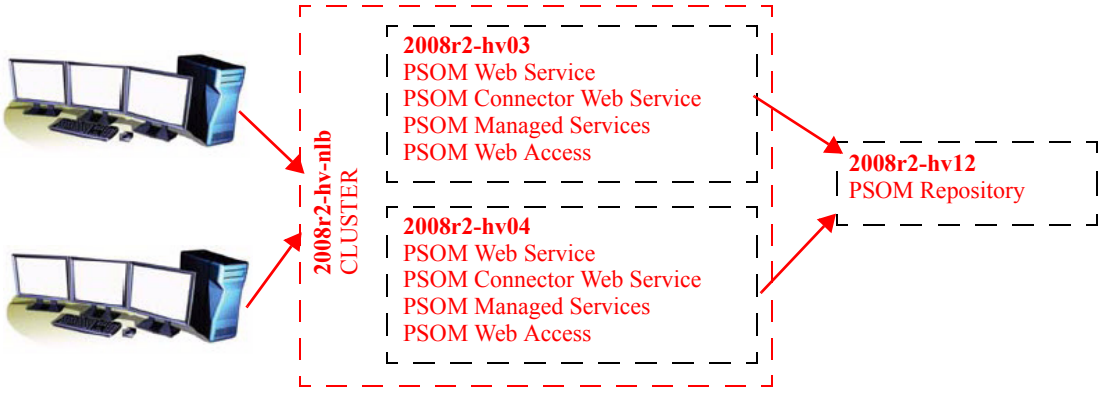
Load Balancing with Microsoft Network Load Balance (NLB)

This appendix explains how to achieve load balancing when deploying PSOM with Microsoft Network Load Balance (NLB) and HyperV virtual machines. To configure redundancy and failover support without using NLB, see Appendix B, "Redundancy and Failover without Clusters." See the Microsoft website for more information about NLB on Windows 2008 R2.

Microsoft Network Load Balance (NLB) can be useful for load balancing across PSOM Web Services as well as PSOM Web Access instances. The scenario presented in this chapter uses 3 HyperV virtual machines on Windows 2008 R2 servers: 2008r2-hv03, 2008r2-hv04, and 2008r2-hv12.

PSOM Repository is installed on 2008r2-hv12. PSOM Web Service, PSOM Connector Web Service, PSOM Managed Services, and PSOM Web Access are installed on 2008r2-hv03 and 2008r2-hv04; both of these virtual machines point to the PSOM Repository on 2008r2-hv12.

Microsoft Network Load Balance must be enabled on the 2008r2-hv03 and 2008r2-hv04 virtual machines. To use NLB in a HyperV virtual machine, you must check the **Enable spoofing of MAC addresses** option in the virtual machine's network adaptor configuration. After creating an NLB Cluster—2008R2-hv-nlb—add the 2008r2-hv03 and 2008r2-hv04 virtual machines to the Cluster. Then point the PSOM Operation Console or Web Access to the Cluster.

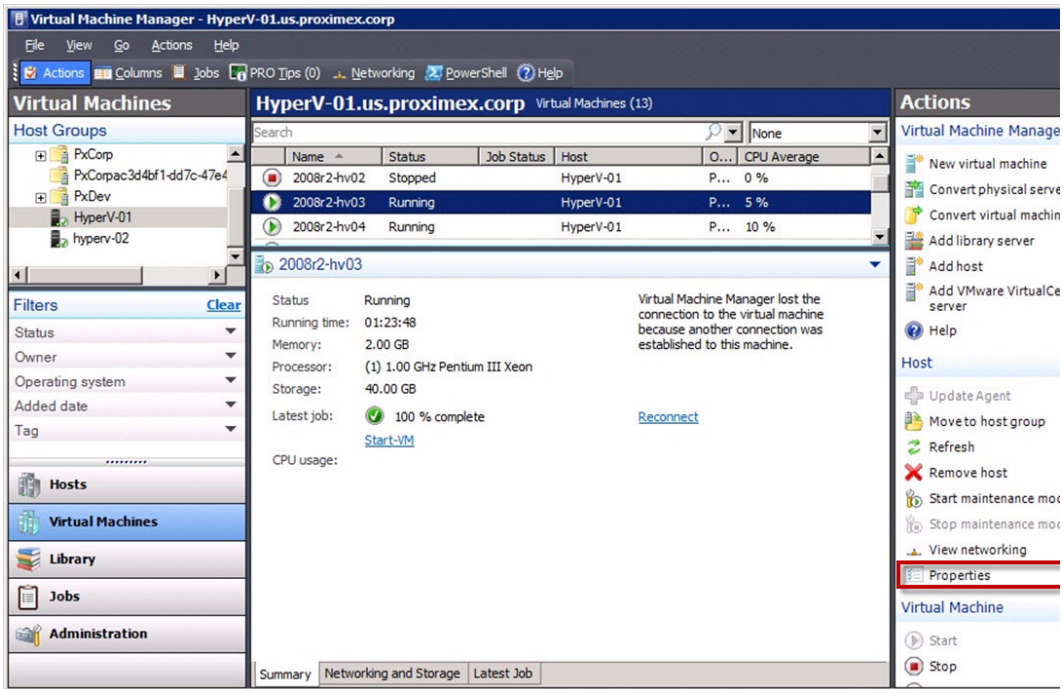


You can also place only the PSOM Web Service on nodes in an NLB Cluster, and then point PSOM Consoles, PSOM Managed Services, and PSOM Web Access to the NLB Cluster.

To set up the NLB Cluster, follow these steps:

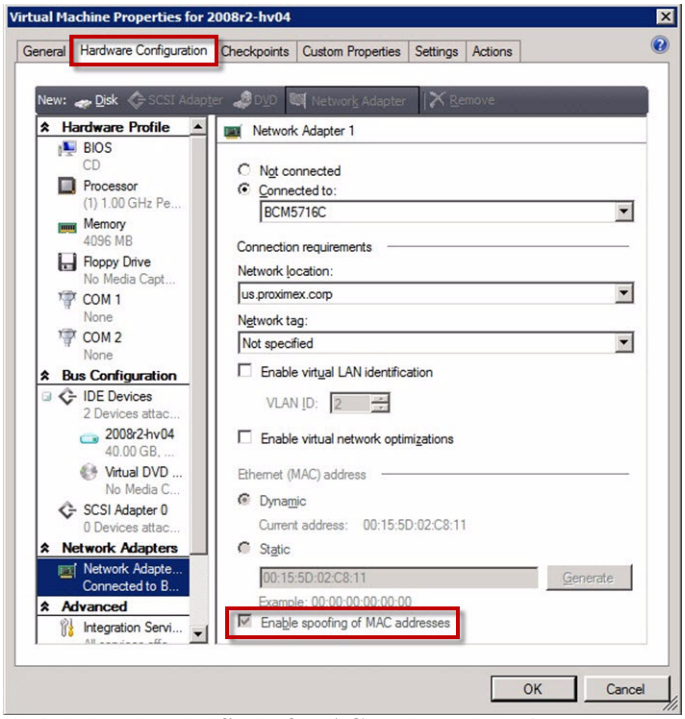
Procedure

Step 1 Launch the Virtual Machine Manager.



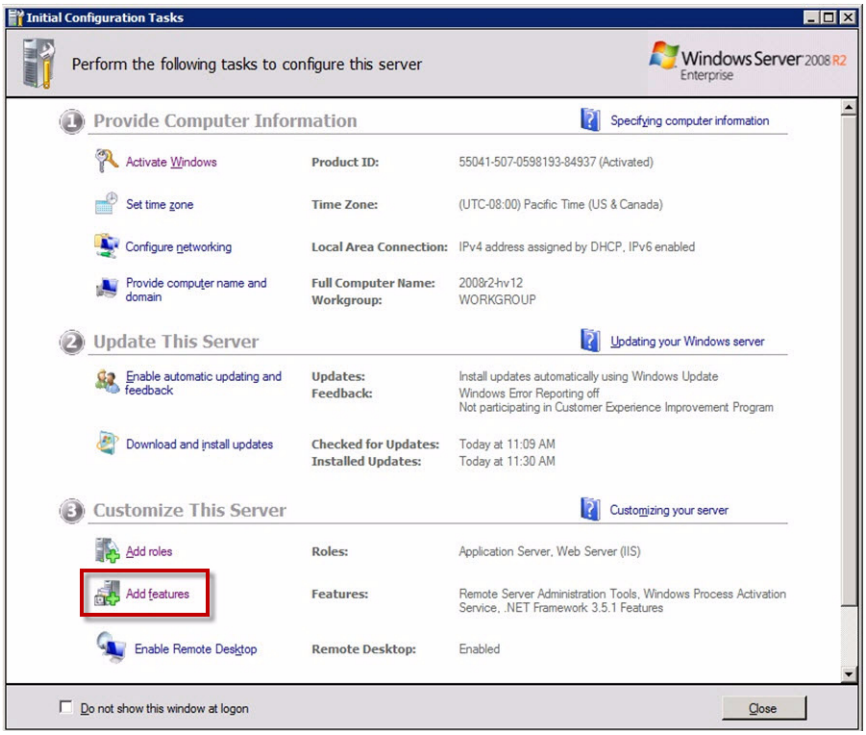
Step 2 Select the virtual machine and select **Properties** in the right pane.

Step 3 Click the **Hardware Configuration** tab.

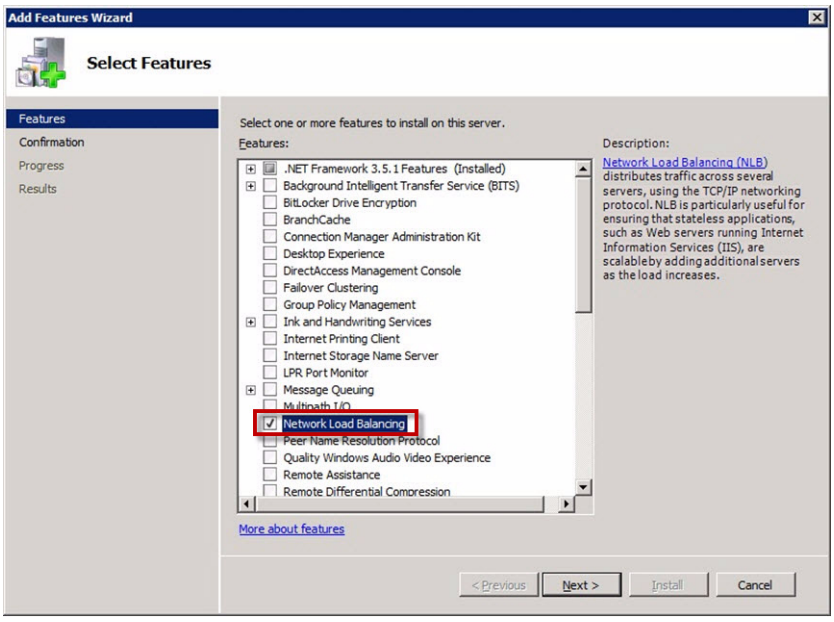


Step 4 Check the **Enable spoofing of MAC addresses** option.

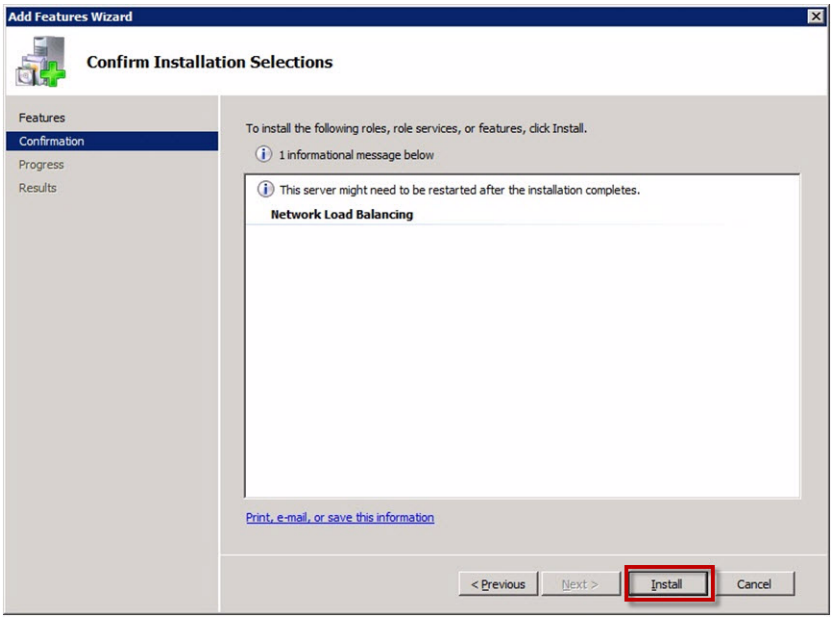
Step 5 Launch Windows 2008R2 Server Manager.



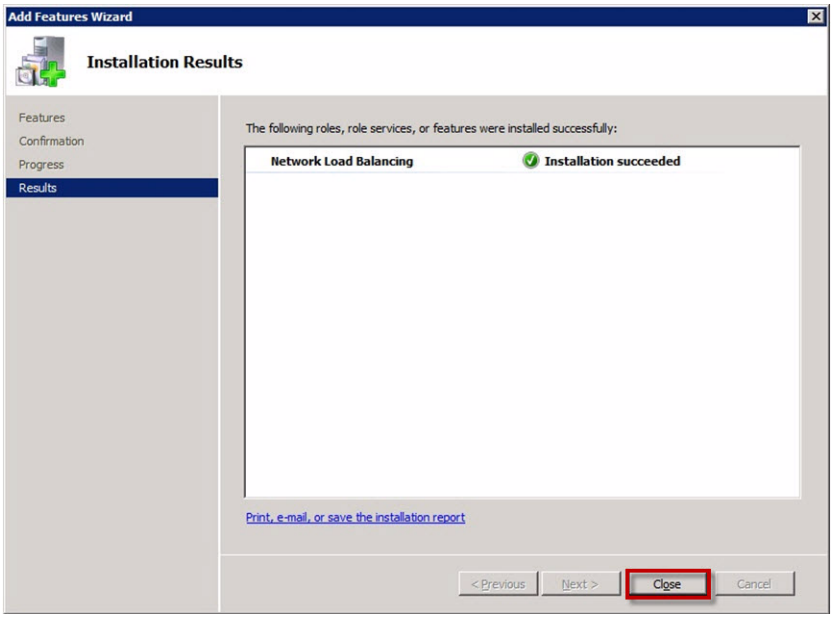
Step 6 Click **Add features**.



Step 7 Select **Network Load Balancing** from the list of features and click **Next**.

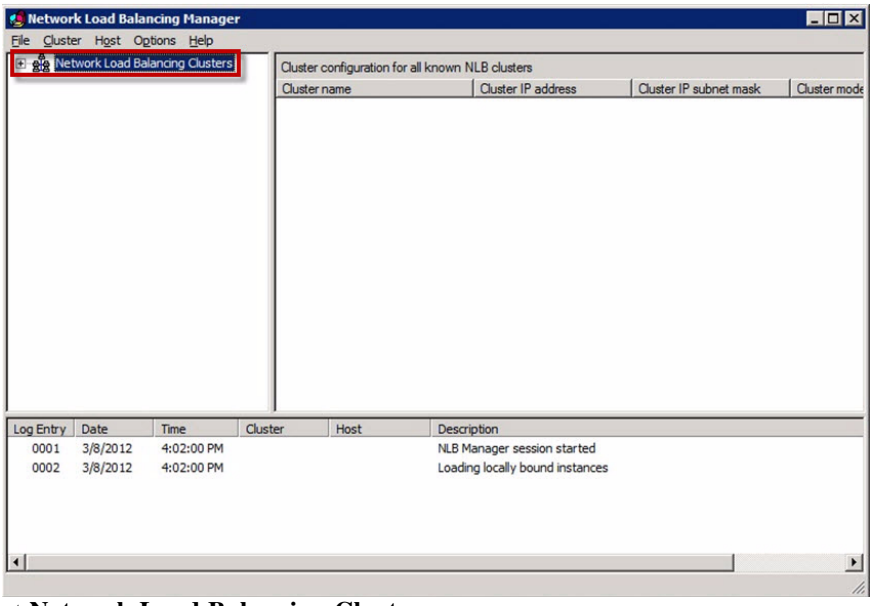


Step 8 Click **Install**.



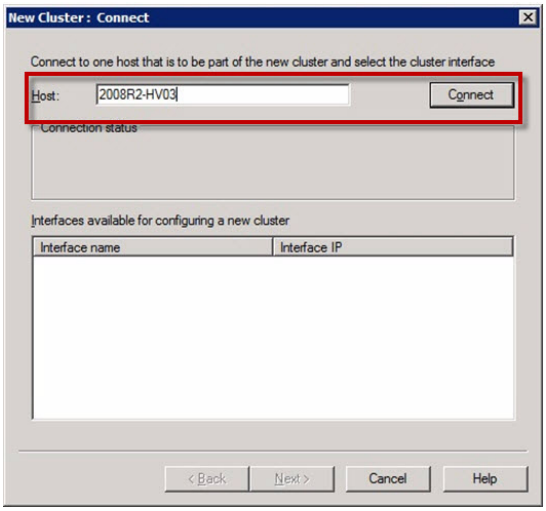
Step 9 When installation completes, click **Close**.

Step 10 Launch the Network Load Balancing Manager.

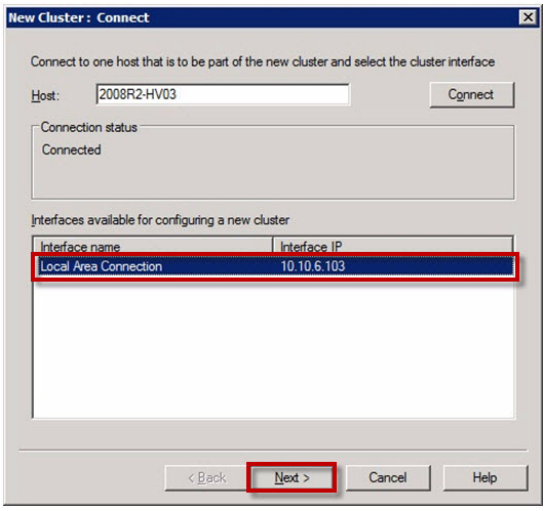


Step 11 Select **Network Load Balancing Clusters**.

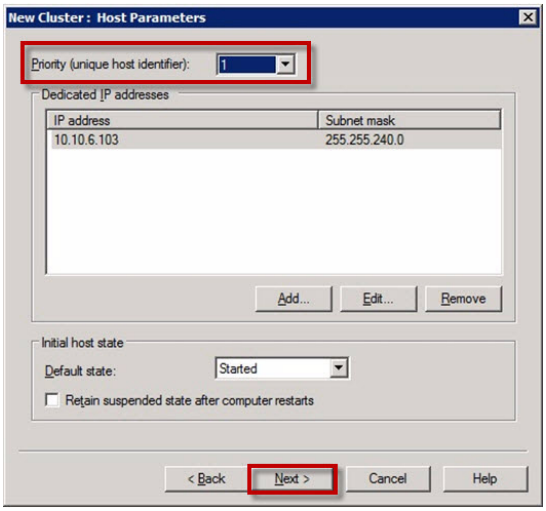
Step 12 Right-click and select **New Cluster**.



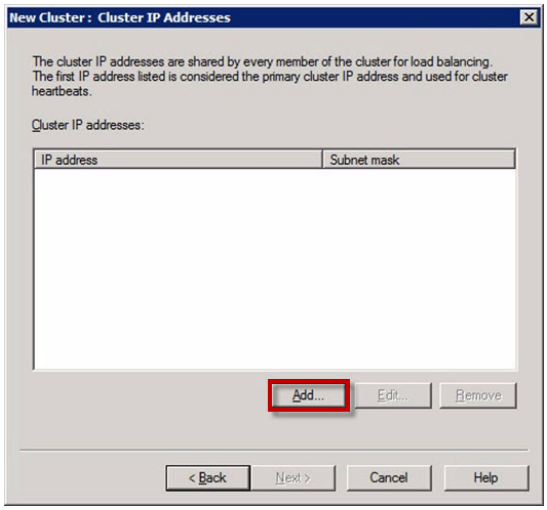
Step 13 Enter a host name to add to the cluster in the **Host** field and click **Connect**.



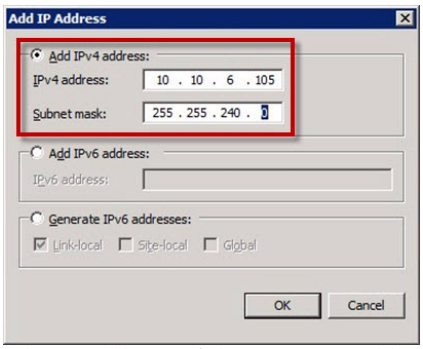
Step 14 The new host appears in the Interfaces area. Click **Next**.



Step 15 Select a priority to assign to the host from the **Priority** field and click **Next**.



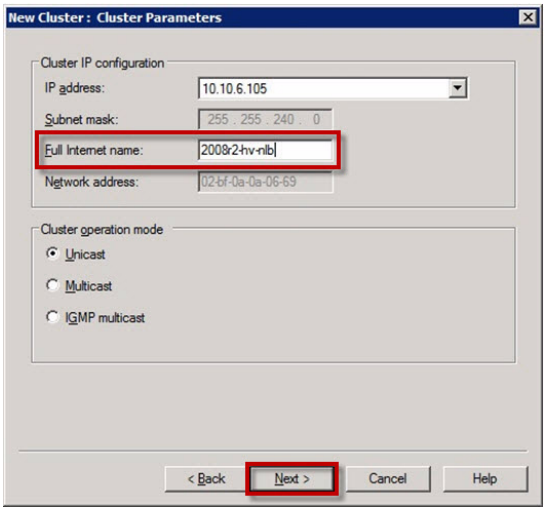
Step 16 Click **Add** to add an IP address to the Cluster.



Step 17 Enter the IP address of the server to add to the Cluster in the **IPv4 address** field.

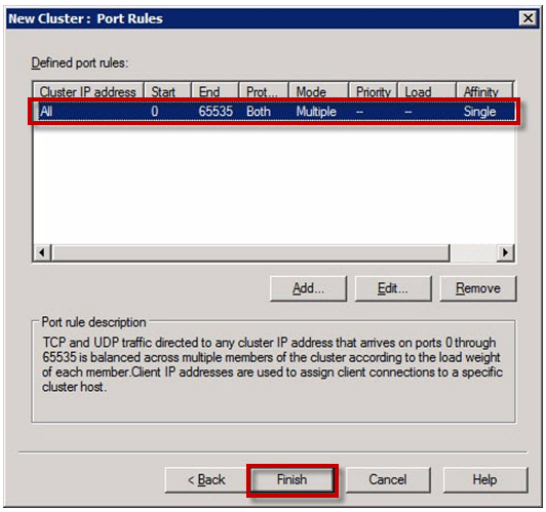
Step 18 Enter the subnet mask of the server to add to the Cluster in the **Subnet mask** field.

Step 19 Click **OK**.



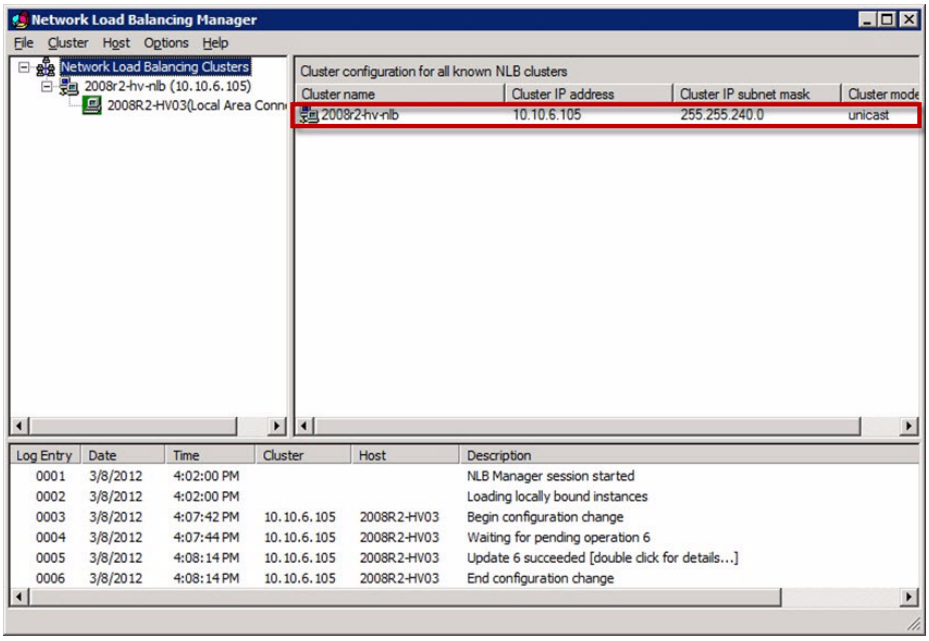
Step 20 Enter the full internet name of the server to add to the Cluster in the **Full Internet name** field.

Step 21 Click **Next**.

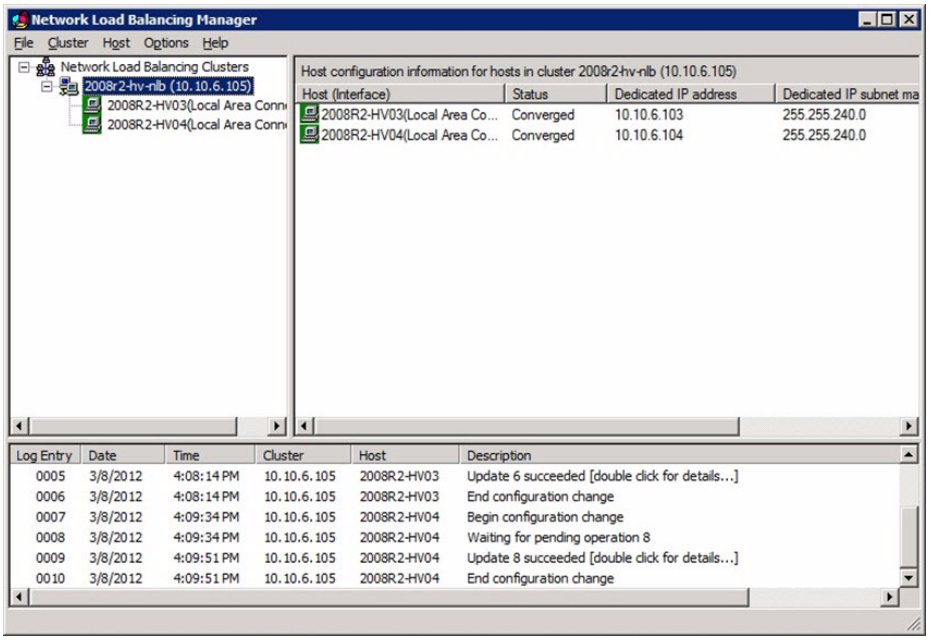


Step 22 Accept the default port rule and click **Finish**.

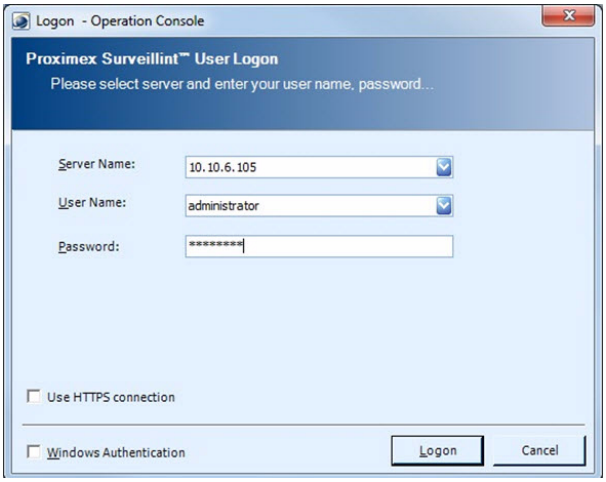
The host is added into the newly created Cluster.



Step 23 Add another host into Cluster and the window appears similar to the following.



Step 24 Launch PSOM Operation Console. In the Logon window, enter the IP address of the Cluster in the **Server Name** field.



When launching the Web Console, the URL should point to the IP address of the Cluster. For example: http://10.10.6.105/PxWebAccess/Logon

APPENDIX D

Installing PSOM on an NEC ExpressCluster

This appendix explains how to install PSOM on an NEC ExpressCluster.

This appendix includes these sections:

Prerequisites

Install the NEC ExpressCluster on two different nodes that each have a share drive. For example, install node A with share drive M for cluster, and node B with share drive N for data.

Note PSOM requires MSSQLSERVER and SQLSERVERAGENT services to be clustered. Others can be left as is.

Configuring SQL Server on ExpressCluster Nodes

Procedure

Step 1 Install MS SQL Server on both ExpressCluster nodes separately.

Step 2 Create a Data folder on one of the nodes in a shared drive; for example, **M:\Data**. This can be used to store the database files.

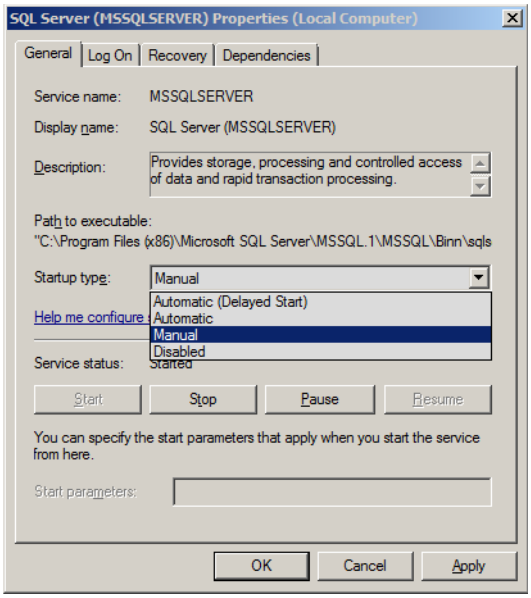
Step 3 Change SQL Server services to use manual startup:

a. Select **Start > Run > services.msc** to launch the ExpressCluster Service Manager.

b. Select **SQL Server (MSSQLSERVER)** and click **Stop**.

c. Double-click the **SQL Server (MSSQLSERVER)** service.

d. In the SQL Server (MSSQLSERVER) Properties window, select **Manual** from the **Startup type** field.



e. Click **Apply** and **OK**.

f. Repeat instructions for the SQL Server Agent service.

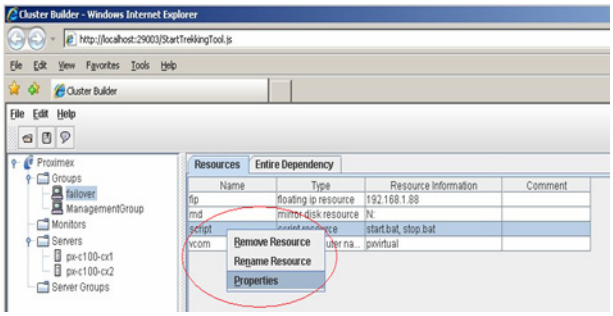
Step 4 Update ExpressCluster start and stop scripts to include SQL Server services.

a. Select **Start > Run > services.msc** to launch the Cluster Service Manager.

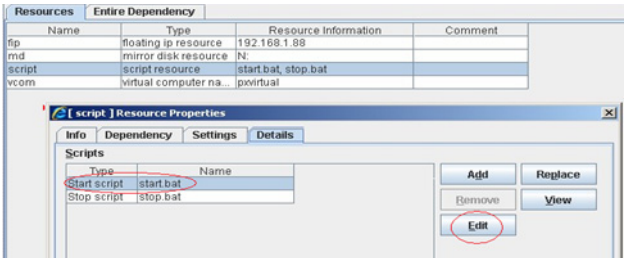
b. Click **Start Builder** to open the Cluster Builder.

c. In the left pane of the Cluster Builder window, select **PSOM > Groups > Failover**.

d. In the right pane, click the **Resources** tab, right-click **script**, and select **Properties** from the popup menu.



The [script] Resource Properties window appears.



e. Select **start script** and click **Edit** to open the script in Notepad.

f. Add the following code to the :Failover and :Normal sections:

```
armload SQL /s /a /r 3 /fov MSSQLSERVER
armload SQLA /s /a /r 3 /fov SQLSERVERAGENT
```

g. Save the script file and click **Apply** in the [script] Resource Properties window.

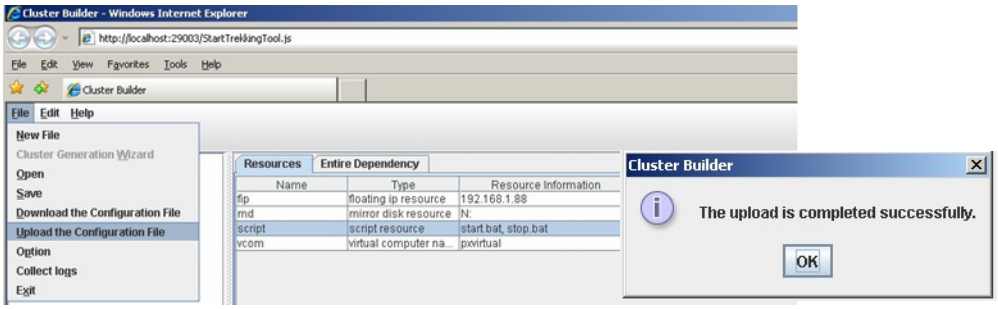
h. Select **stop script** and click **Edit** to open the script in Notepad.

i. Add the following code to the :Failover and :Normal sections:

```
armload SQL /s /a /r 3 /fov MSSQLSERVER
armload SQLA /s /a /r 3 /fov SQLSERVERAGENT
```

j. Save the script file and click **Apply** and **OK** in the [script] Resource Properties window.

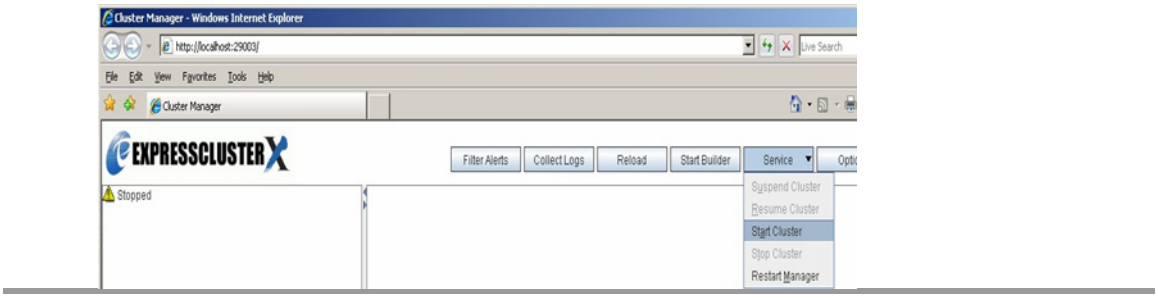
k. In the Cluster Builder window, select **File > Upload the Configuration File** to upload these changes.



Step 5 Start the Cluster Service using the ExpressCluster Manager.

a. Navigate a web browser to http://*localhost*:29003 where *localhost* is the name of one of the cluster nodes; for example, http://px-c100-cx1:29003/.

b. Select **Start Cluster** from the **Service** drop-down menu.



Installing/Configuring PSOM Repository on an ExpressCluster

Install the PSOM Repository on the active ExpressCluster node, specifying the path for the ProximexDB file to be the Data folder created on the shared drive. This ensures that the database functions on the clustered node. Then failover to the other ExpressCluster node and re-run the PSOM Repository installation on the second node.

Note The PSOM Repository is installed on both nodes so that SQL Server can locate the database correctly during failover. When performing an upgrade for ProximexDB, simply install PSOM Repository on the active node. Since PSOM Repository is already installed on the shared node it will be recognized by the second node when during failover. Do not reinstall PSOM Repository on the second node. Reinstalling or upgrading on the second node could cause overwriting of the upgraded PSOM Repository database.

Installing/Configuring PSOM Web Service and Connector Web Service on an ExpressCluster

Installing IIS on a virtual drive

For IIS 6.0, you can perform an unattended installation of IIS after creating an answer file. Update the PathWWWRoot to be equal to N:, where N: is the virtual drive.

See the following URL for instructions on generating an answer file:

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/efefcb53-b86e-4cac-9b4b-fcf5f1145aa9.mspx?mfr=true

For IIS 7.0 on Windows Server 2008, you must install the Web Service to the C: drive. To locate IIS on a different drive you must move it after installation.

See the following URL for instructions on moving IIS 7.0 to a different drive after installation:

http://blogs.iis.net/thomad/archive/2008/02/10/moving-the-iis7-inetpub-directory-to-a-different-drive.aspx

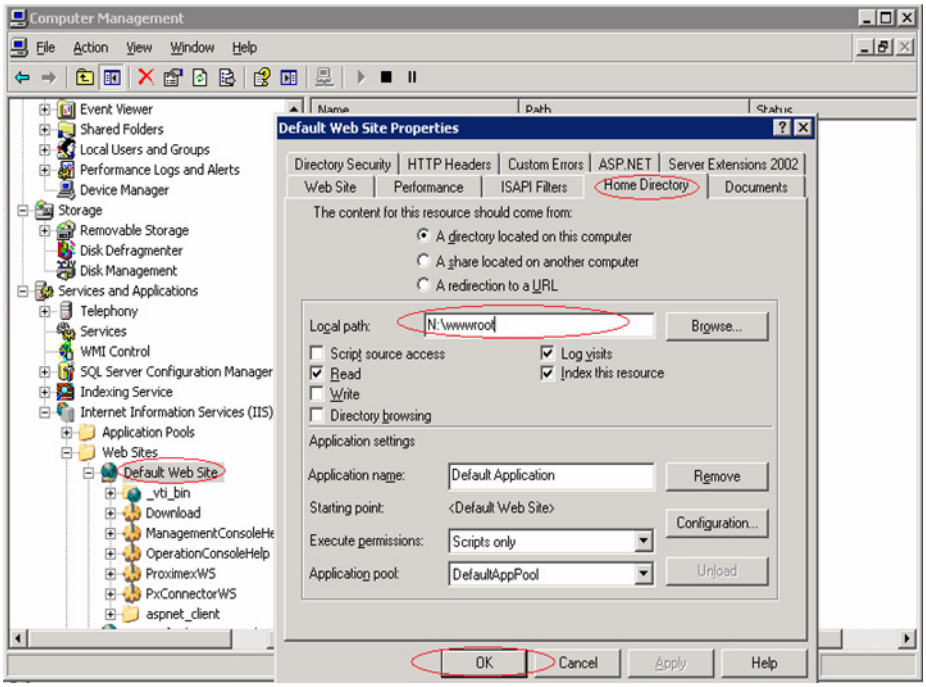
You can also move the IIS 7.0 WWWroot to a virtual drive after installation.

Procedure

Step 1 Select **Computer Management > Internet Information Services (IIS) Manager > Websites > Default Web Site**.

Step 2 Right-click **Default Web Site** and select **Properties**.

Step 3 Click the **Home Directory** tab and update the **Local Path** field to the location of the shared folder; for example, N:\wwwRoot.



Step 4 Click **OK** and repeat steps on the second Cluster node.

Configuring IIS on the ExpressCluster

On each of the ExpressCluster nodes, stop the World Wide Web Service and change its startup mode to manual.

Procedure

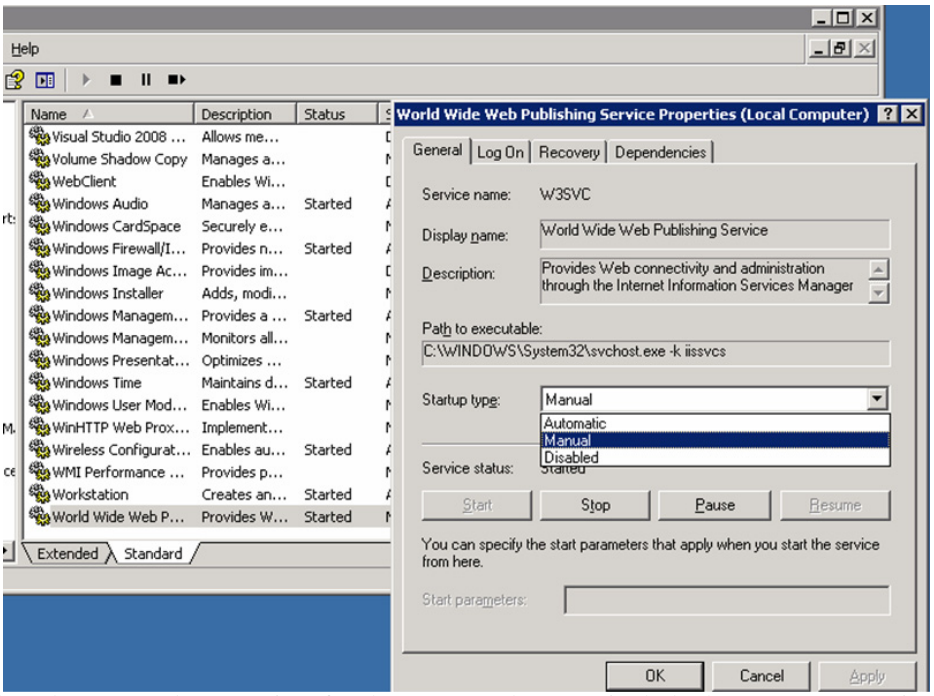
Step 1 Select **Start > Run > services.msc**.

Step 2 Select **World Wide Web Service (w3svc)** and click **Stop the service**.

Step 3 Double-click the **World Wide Web Service**.

Step 4 Select **Manual** from the **Startup type** field in the Properties window.

Step 5 Click **OK** to save changes.

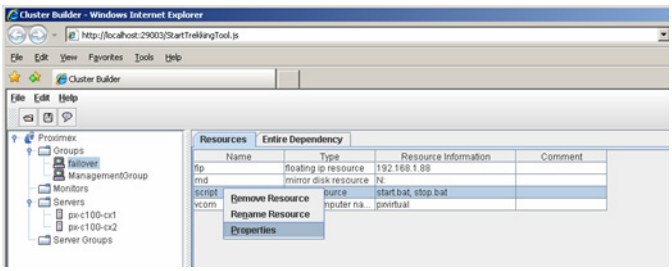


Step 6 Update the start and stop scripts for the ExpressCluster to include the necessary services.

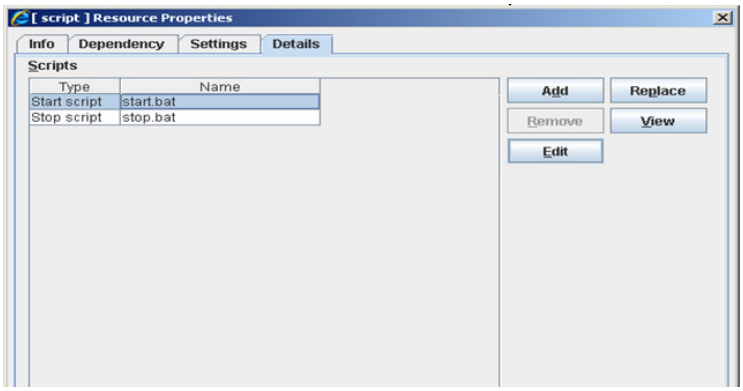
a. Open the Cluster Builder window by navigating to the following URL in a web browser: http://localhost:29003/StartTrekkingTool.js

b. In the left pane, select **PSOM(*Cluster name*) > Groups > Failover**.

c. In the right pane, right-click **script** and select **Properties**.



d. Click the **Details** tab and click **Start script**.



e. Click **Edit**.

f. Add the following code to the end of the :NORMAL and :FAILOVER scripts:

```
armload IIS /s /a /r 3 /fov W3SVC
```

```
rem ****************************************
rem Normal Startup process
rem ****************************************
:NORMAL
armload SQL /s /a /r 3 /fov MSSQLSERVER
armload SQLA /s /a /r 3 /fov SQLSERVERAGENT
armload IIS /s /a /r 3 /fov W3SVC
```

g. Save and close the file.

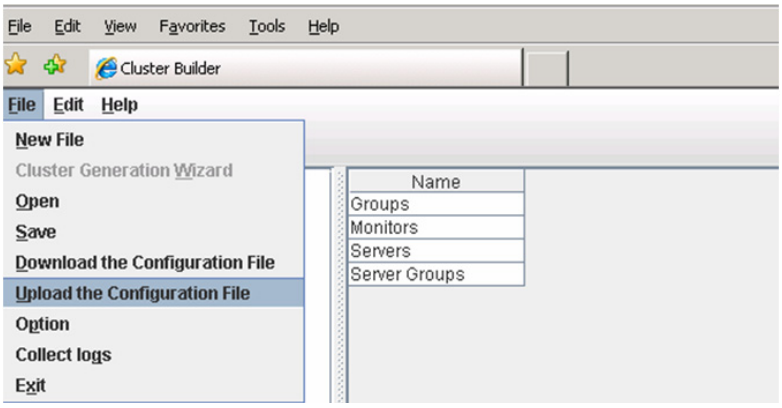
h. Edit **Stop script** to append the following code to the end of the :Normal and :Failover scripts:

```
armkill IIS
```

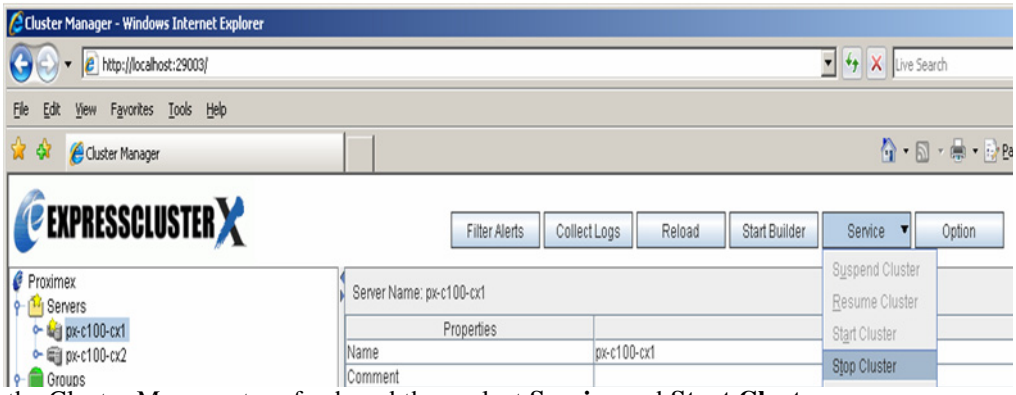
i. Save and close the file.

j. Apply these changes in the Resource Properties window.

k. In the Cluster Builder, select **File > Upload the Configuration File** to save and upload the changes.



l. Stop the ExpressCluster service by selecting **Service** and **Stop Cluster** in the Cluster Manager.



Step 7 Wait for the Cluster Manager to refresh and then select **Service** and **Start Cluster**.

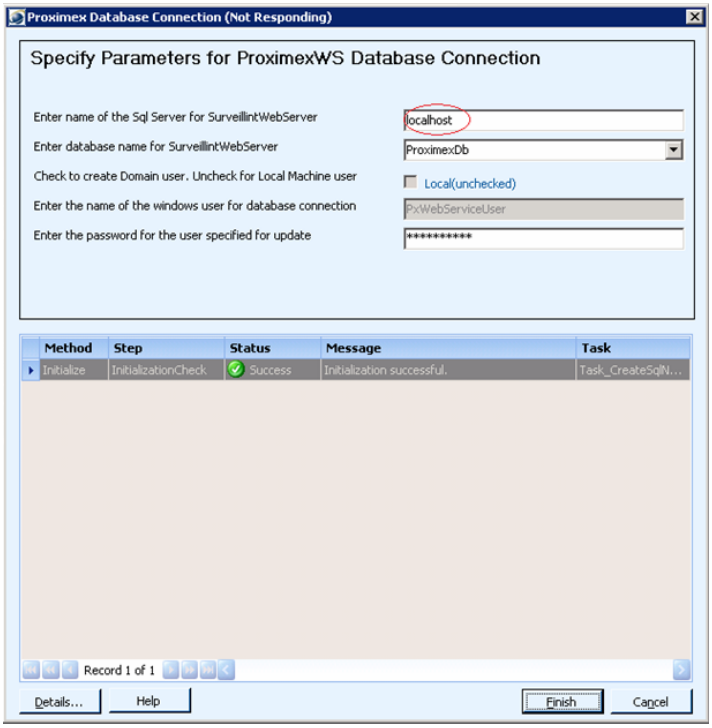
Installing PSOM Web Service on an ExpressCluster

Procedure

Step 1 Install the following PSOM components on each of the ExpressCluster nodes:

- PSOM Prerequisite (PxWizardPrereq.msi)
- PSOM Web Service (PxWebServiceSetup.msi | PxWebServiceSetup.bat)
- PSOM Connector Web Service (PxConnectorWSSetup.msi | PxConnectorWSSetup.bat)

Step 2 During the PSOM Web Service installation, enter **localhost** in the **Enter the name of the Sql Server for Surveillint Web Server** field instead of the name of the ExpressCluster node. This will ensure that PSOM Web Service remains operational during failover between ExpressCluster nodes.



Step 3 Verify that the PSOM Web Service folder ProximexWS and PxConnectorWS are installed in a virtual drive under the N:\wwwroot folder.

Note The PSOM Web Service database configuration will require restarting the IIS Service which will cause the ExpressCluster to failover. To avoid multiple failovers you can shut down the second node while installing the first node, and vice versa.

Installing and Configuring PSOM Managed Services on an ExpressCluster

To set up PSOM 5.1 Managed Services on an NEC ExpressCluster's Virtual Server, follow these steps:

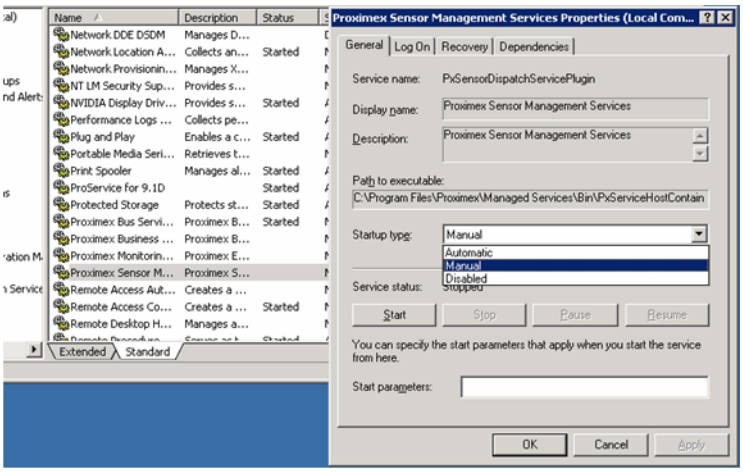
Procedure

Step 1 Install all PSOM components on each of the ExpressCluster nodes; use the default path.

Step 2 From the Service Manager, stop all PSOM Services and change the Startup type to Manual. Perform these steps for these services:

- PSOM Business Logic Core Services—PxBusinessLogicService
- PSOM Bus Services—PxBusServices
- PSOM Caching Services—PxCacheServices
- PSOM Monitoring Logic Services—PxPreAlertService

- PSOM Sensor Management Services—PxSensorDispatchServicePlugin



Step 3 Create a folder to store PSOM Services data files in the ExpressCluster's virtual drive. For example, create ***N:*\Program Files\Cisco PSOM\ Managed Services\Bin** where *N:* is the Cluster's virtual drive.

Step 4 Update the Config path for PSOM Services in the Windows Registry to see the ExpressCluster's virtual path.

- Update the string ManagedServicesConfigDataPath in the HKEY_LOCAL_MACHINE\SOFTWARE\Proximex Corp key to N:\Program Files\Cisco PSOM \Managed Services\Bin
- In a Windows 64-bit system, the Registry key to be updated is HKLM\SOFTWARE\Wow6432Node\Proximex Corp\ManagedServicesConfigDataPath

Repeat this procedure on both ExpressCluster nodes.

Step 5 Move PSOM XML files from C:\Program Files\Proximex\Managed Services\Bin to N:\Program Files\Proximex\Managed Services\Bin folder, specifically the following XML files:

- PxBusinessLogicService.logger.xml
- PxBusinessLogicService.xml
- PxBusServices.logger.xml
- PxBusServices.xml
- PxCommonDbWsConfig.xml
- PxCommonLoggerConfig.logger.xml
- PxPreAlertService.logger.xml
- PxPreAlertService.xml
- PxSensorDispatchServicePlugin.logger.xml
- PxSensorDispatchServicePlugin.xml

Step 6 Launch the Computer Management window, select **Services and Applications > Services**.

Step 7 For each PSOM Service, stop the service and change its startup type to manual, including: PxBusinessLogicService, PxBusServices, PxCachingServices, PxPreAlertService, PxSensorDispatchServicePlugin.

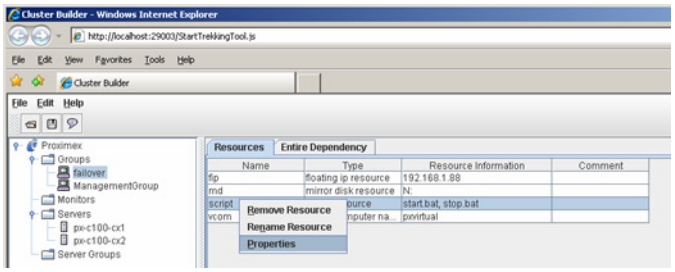
Step 8 Stop the IIS service (World Wide Publishing service) and change its startup type to manual.

Step 9 Update the ExpressCluster's start and stop scripts to include the PSOM Managed Services and the IIS Service.

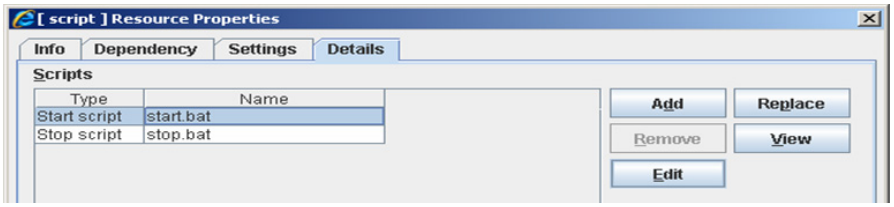
a. Open the Cluster Builder by navigating a web browser to http://localhost:29003/StartTrekkingTool.js.

b. Select **PSOM (*Cluster name*) > Groups > Failover**.

c. Right-click **script** and select **Properties**.

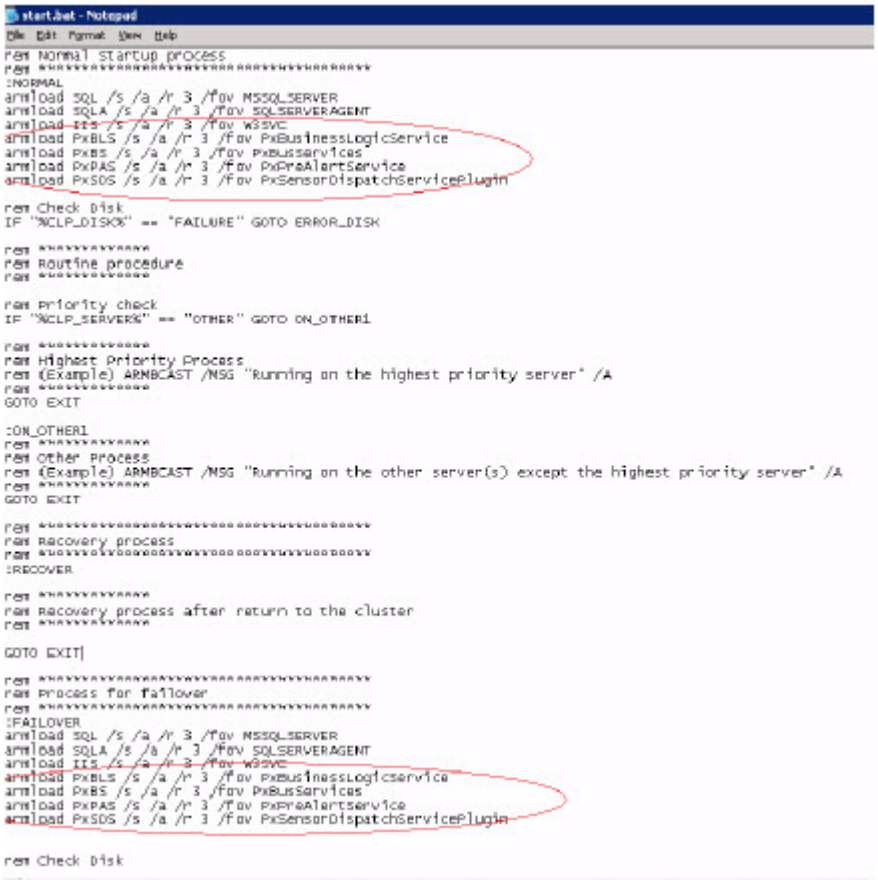


d. In the [script] Resource Properties window, select the **Details** tab, select **Start script**, and click **Edit**.



e. Add the following code after the :NORMAL and :FAILOVER scripts:

```
armload PxBLS /s /a /r 3 /fov PxBusinessLogicService
armload PxBS /s /a /r 3 /fov PxBusServices
armload PxPAS /s /a /r 3 /fov PxPreAlertService
armload PxSDS /s /a /r 3 /fov PxSensorDispatchServicePlugin
```

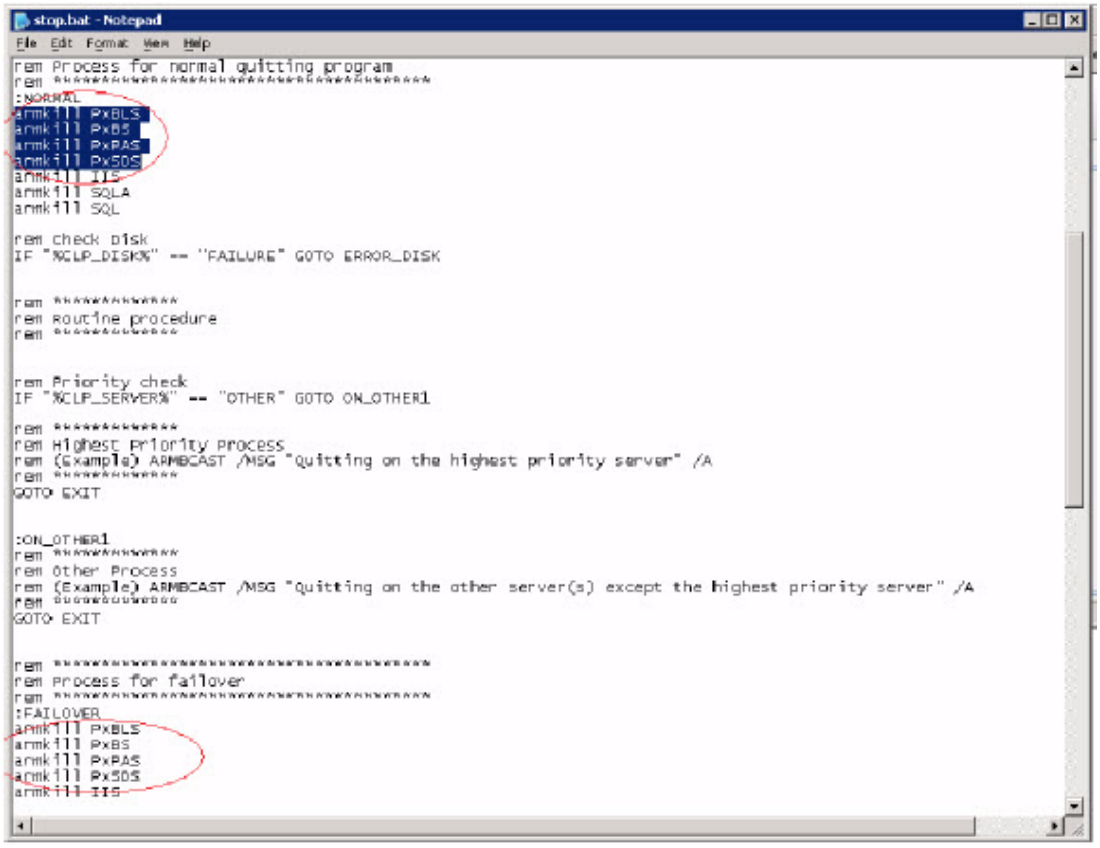


f. Save and close the script file.

g. In the [script] Resource Properties window, select the **Details** tab, select **Stop script**, and click **Edit**.

h. Add the following code after the :NORMAL and :FAILOVER scripts:

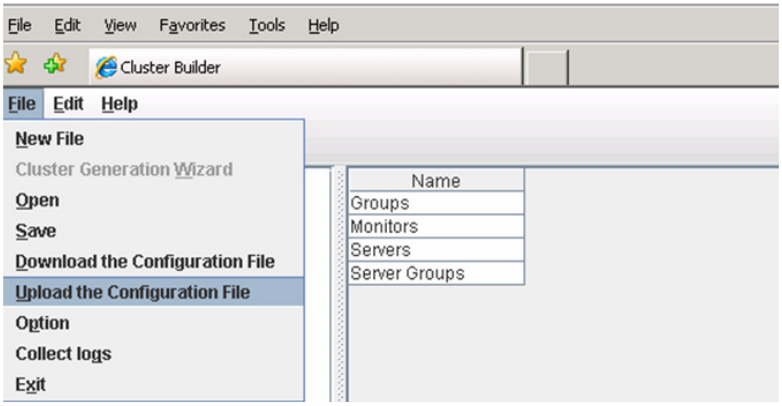
```
armkill PxBLS
armkill PxBS
armkill PxPAS
armkill PxSDS
```



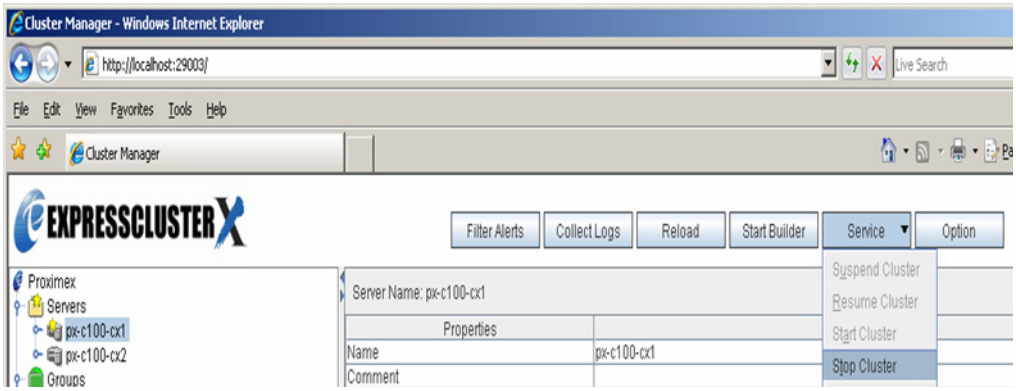
i. Save and close the script file.

j. Apply these changes in the Resource Properties window.

k. In the Cluster Builder, select **File > Upload the Configuration File** to save and upload the changes.



l. Stop the ExpressCluster service by selecting **Service** and **Stop Cluster** in the Cluster Manager.



m. Wait for the Cluster Manager to refresh and then select **Service** and **Start Cluster**.

Installing PSOM 5.1 Consoles on an ExpressCluster

Install the PSOM 5.1 Consoles on both ExpressCluster nodes. PSOM Consoles are not cluster-aware and can be installed on an ExpressCluster node just the same as it is installed on any non-ExpressCluster machine.

When connecting to the PSOM Web Service for the ExpressCluster, the name of the PSOM Web Service should be the name of the virtual server and not the name of the ExpressCluster node. While providing the active ExpressCluster node's name will enable connection to the PSOM Repository, once the ExpressCluster fails over to the other node, PSOM Consoles will no longer be able to access the PSOM Repository.

Conversely, if the PSOM Consoles are logged in to the virtual server they will automatically be redirected to the alternate ExpressCluster node during failover.

Note When configuring PSOM Integration Modules, the PSOM Consoles must be connected to the active ExpressCluster node rather than the virtual server. Otherwise, the Integration Module functionality is disabled in the Administration Console.

The Integration Module functionality is enabled in the Administration Console because the PSOM Consoles are connected to localhost which is the active ExpressCluster node.

Note Every Integration Module configuration requires the IIS Service to be restarted which will cause the ExpressCluster to failover. To avoid multiple failovers during configuration, shutdown the second ExpressCluster node while performing configuration. Another approach is to use the Plugin Pages to configure all Integration Modules and then restart the IIS Service after configuration is complete.

Uninstalling PSOM

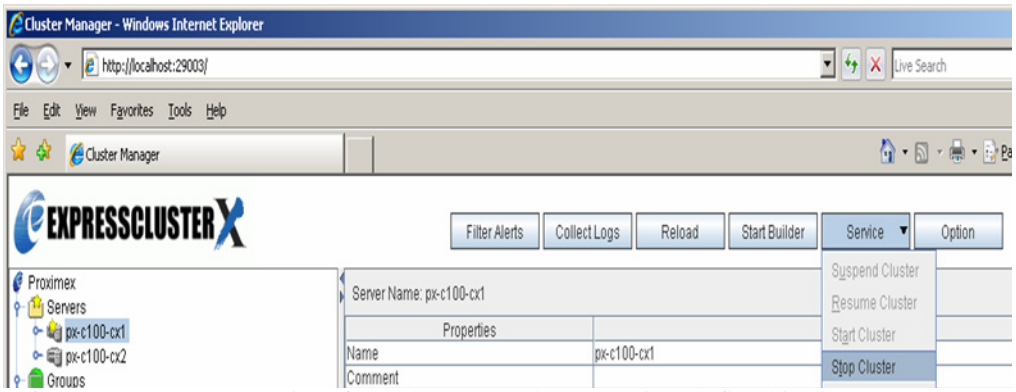
To uninstall PSOM from an ExpressCluster, follow these steps:

Procedure

Step 1 Stop the ExpressCluster service using the Cluster Manager.

a. Navigate to the following URL from a web browser: **http://localhost:29003**

b. Stop the ExpressCluster service by selecting **Service** and **Stop Cluster** in the Cluster Manager.

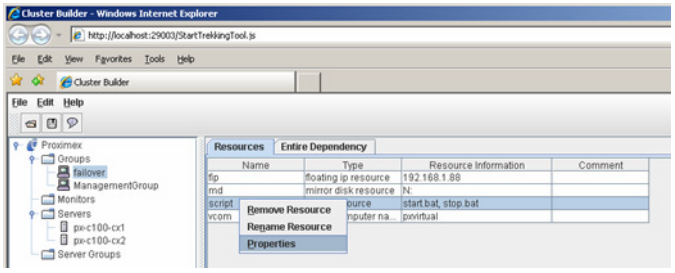


Step 2 Remove references to PSOM Services from the **stop** and **start** scripts defined in the ExpressCluster.

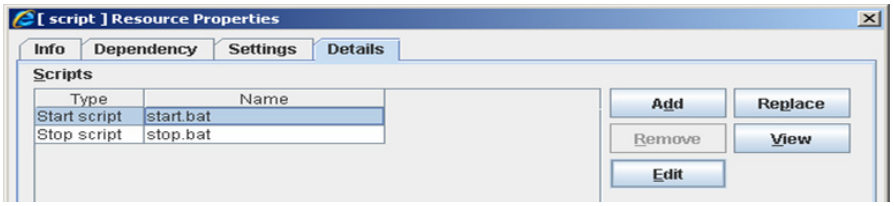
a. Open the Cluster Builder by navigating a web browser to http://localhost:29003/StartTrekkingTool.js.

b. Select **PSOM (*Cluster name*) > Groups > Failover**.

c. Right-click **script** and select **Properties**.



d. In the [script] Resource Properties window, select the **Details** tab, select **Start script**, and click **Edit**.



e. Remove code references from the end of the :NORMAL and :FAILOVER scripts.

```
armload PxBLS /s /a /r 3 /fov PxBusinessLogicService
armload PxBS /s /a /r 3 /fov PxBusServices
armload PxPAS /s /a /r 3 /fov PxPreAlertService
armload PxSDS /s /a /r 3 /fov PxSensorDispatchServicePlugin
```

f. Save and close the script file.

g. In the [script] Resource Properties window, select the **Details** tab, select **Stop script**, and click **Edit**.

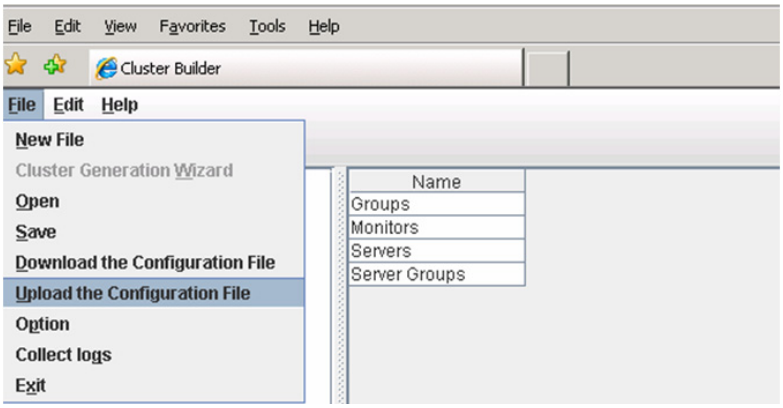
h. Remove code references from the end of the :NORMAL and :FAILOVER scripts.

```
armkill PxBLS
armkill PxBS
armkill PxPAS
armkill PxSDS
```

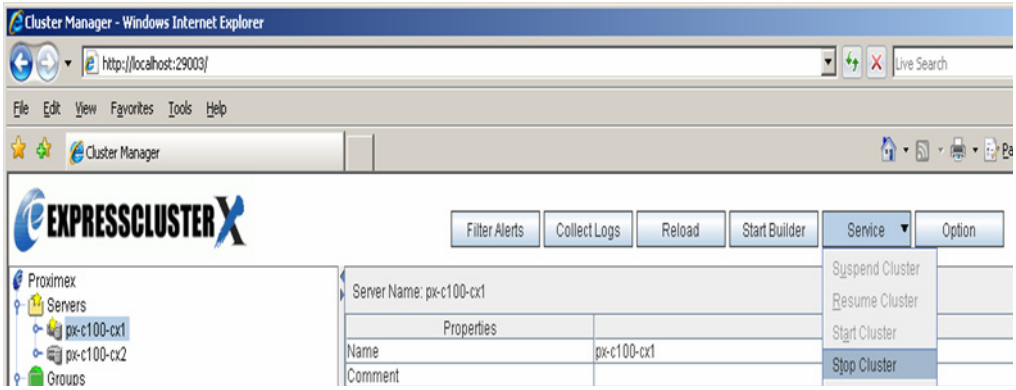
i. Save and close the script file.

j. Apply these changes in the Resource Properties window.

k. In the Cluster Builder, select **File > Upload the Configuration File** to save and upload the changes.



l. Stop the ExpressCluster service by selecting **Service** and **Stop Cluster** in the Cluster Manager.



m. Wait for the Cluster Manager to refresh and then select **Service** and **Start Cluster**.

Step 3 Uninstall the PSOM Services from both ExpressCluster nodes.

Step 4 Failover to the ExpressCluster node that was used to install PSOM Repository.

Step 5 Uninstall PSOM Repository.

APPENDIX E

Setting Up Database Mirroring for PSOM Repository

This appendix explains why you would want to set up database mirroring for PSOM Repository, and walks through the steps for doing so.

This appendix includes these sections:

Overview

When PSOM depends upon a single SQL Server to host the PSOM Repository, there is risk that SQL Server or the machine hosting it will fail, causing all operations dependent upon the PSOM Repository to fail. One way to avoid this issue and provide high availability of the PSOM Repository is database mirroring.

Although there are other approaches for ensuring high availability of the PSOM Repository, database mirroring with SQL Server is the recommended approach due to lower SQL Server administration costs and greater equipment flexibility.

- Any hardware that meets requirements for the PSOM Repository can be used for database mirroring, unlike database clustering which requires a shared disk resource (high performance RAID drive) and special licenses for Windows and SQL Server.
- Automated client redirect is supported natively by .NET Data providers for database mirroring.
- Full disaster recovery (Geo-Failover) is supported by database mirroring because active mirrored databases can be instantiated in multiple physical sites (SQLServer1 in San Jose and SQLServer2 in San Francisco).

Furthermore, the PSOM Web Service and PSOM Services offer built-in support for database mirroring should you choose to implement it.

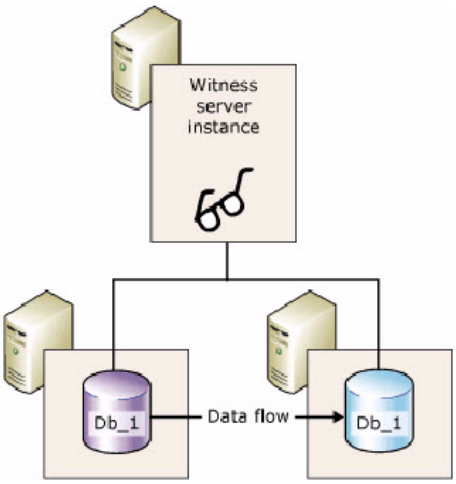
Database Mirroring with PSOM

With PSOM database mirroring, two copies of the PSOM Repository (ProximexDb) are maintained by unique instances of SQL Server (Standard Edition), typically on different machines. One server instance serves the ProximexDb database to PSOM Services and Consoles (the Principal SQL Server). The other instance acts as a hot or warm standby server (the Mirror SQL Server).

PSOM uses a high-safety database mirroring mode which enables automated client redirection by using a "Witness" SQL Server instance in addition to the Primary and Mirror SQL Server instances. The Witness SQL Server can be SQL Server Express, and can reside on the same machine with either the Principal or Mirror SQL Servers.

Unlike the Primary and Mirror SQL Servers, the Witness SQL Server does not serve the database. The Witness SQL Server supports automatic failover by verifying whether the Principal SQL Server is functioning. The Mirror SQL Server initiates automatic failover only if it remains connected to the Witness SQL Server after both have been lost contact with the Principal SQL Server.

This high-safety mode minimizes administrative overhead and minimizes software costs associated with SQL Server Enterprise licensing; the synchronous transactions required by the high-safety mode slightly decrease performance.



Note To enable database mirroring, the ProximexDb uses the full recovery model. Therefore, all bulk operations are fully logged.

Prerequisites for Mirroring PSOM Repository

Before proceeding with the steps in the "Mirroring PSOM Repository" section on page E-3:

- Stop all PSOM Services.
- Close all PSOM Consoles.
- Issue an IISRESET command on all machines with PSOM software to release any existing database connections.
- Use an administrative account with rights to all machines that host SQL Server and sysadmin permissions for all SQL Server instances.

Mirroring PSOM Repository

The overall steps to setting up mirroring for PSOM Repository are:

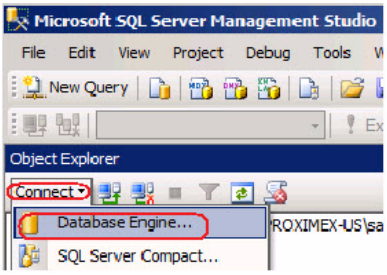
- Add three instances of Microsoft SQL Server on the network: Principal SQL Server, Witness SQL Server and Mirror SQL Server. This is to implement a high-safety mirroring solution. It is recommended that all three instances of Microsoft SQL Server use SQL Server 2008 R2.
- Set Microsoft SQL Server to use a domain account for the service account (all instances). Doing so allows all three instances of SQL Server to communicate with each other to enable verification, data transfer and ultimately failover. Ensure that the domain user has Run-As-Service authority on the Windows machines where SQL Server instances are running.
- Install ProximexDb in the Principal (.) SQL Server (if not already installed).
- Set ProximexDb to use Full recovery mode.
- Execute a full database backup of the ProximexDb database on the Principal SQL Server.
- Copy the database backup file to the Mirror SQL Server.
- Create a new ProximexDb database on the Mirror SQL Server.
- Restore the backup ProximexDb database to the Mirror SQL Server with No Recovery mode.
- Activate mirroring of the ProximexDb database from the Principal SQL Server.

To mirror the PSOM Repository, follow these steps:

Procedure

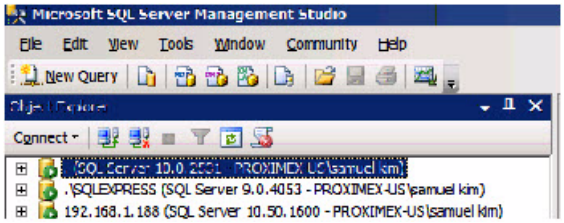
Step 1 Launch Microsoft SQL Server Management Studio.

Step 2 Click **Connect > Database Engine...**.



Step 3 Select the server that houses PSOM Repository and click **Connect**.

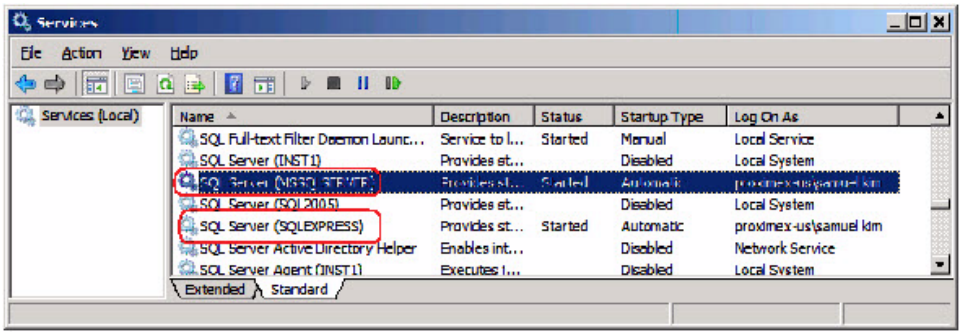
Step 4 Install three instances of Microsoft SQL Server on the network. Shown next, one machine hosts the Witness SQL Server (.\SQLEXPRESS) and Principal SQL Server (.), and another hosts the Mirror SQL Server (192.168.1.188).



Step 5 Set Microsoft SQL Server to use a domain account for the service account.

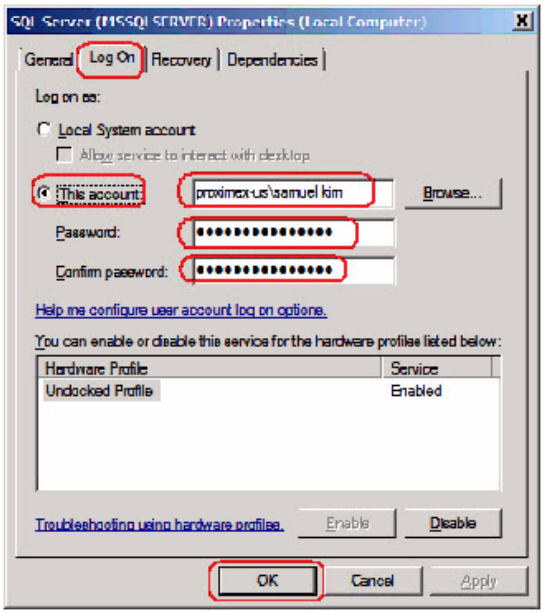
On each Windows machine:

a. Select **Start > Control Panel > Administrative Tools > Services**.



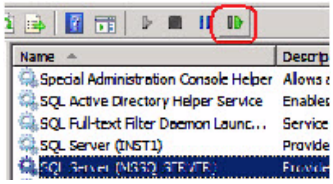
b. Locate and double-click each SQL Server instance in the Services list. In the example shown, the Principal SQL Server and Witness SQL Server are on the same machine. The SQL Server Properties window appears.

c. Click the **Log On** tab, select **This account** and enter the domain user and password in the fields provided. Click **OK**.

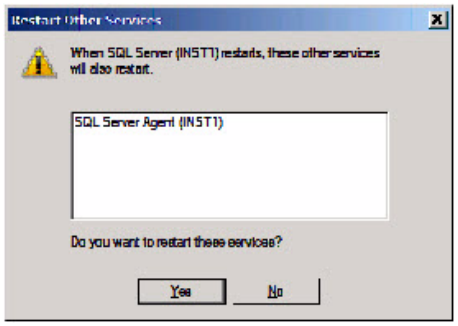


d. Click **OK** when prompted.

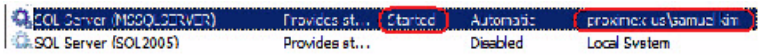
e. Select SQL Server instance in the Services list and click the **Restart** button.



f. Click **Yes** if a message similar to the following appears.



g. Verify that the SQL Server instance and SQL Agent are running under the correct domain user account.



Step 6 Install ProximexDb in the Principal (.) SQL Server (if not already installed). You can restore an existing ProximexDb database as well.

Step 7 Set ProximexDb to use Full recovery mode.

Note You must first close all connections to the ProximexDb database.

a. Close all PSOM Consoles.

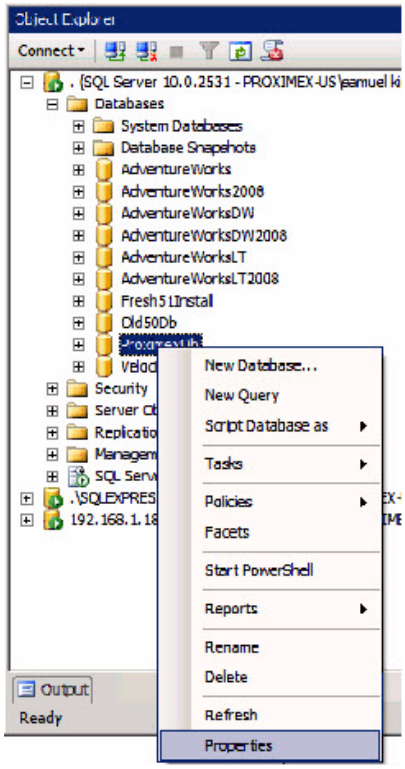
b. Stop all PSOM Services.

c. Restart the IIS Service. Select **Start > Run** and enter the following commands in the Run dialog.

net stop w3svc

net start w3svc

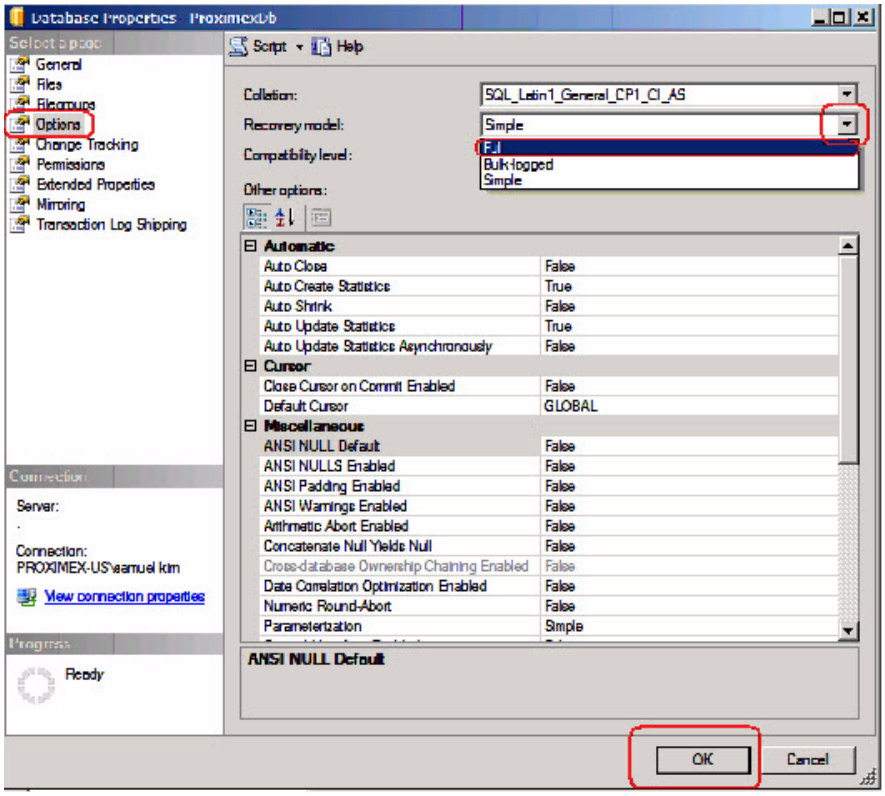
d. From Microsoft SQL Server Management Studio, expand **Databases** under the Principal SQL Server(.). Right click the **ProximexDb** database and select **Properties**.



e. Click **Options** in the left pane of the Database Properties dialog.

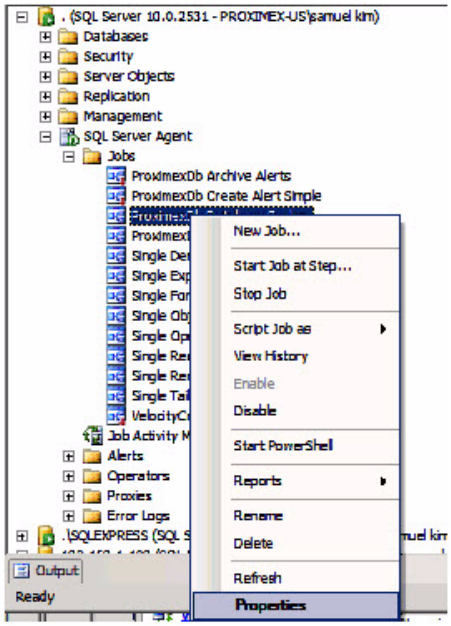
f. From the **Recovery Model** field on the **Options** tab, choose **Full**.

g. Click **OK**.

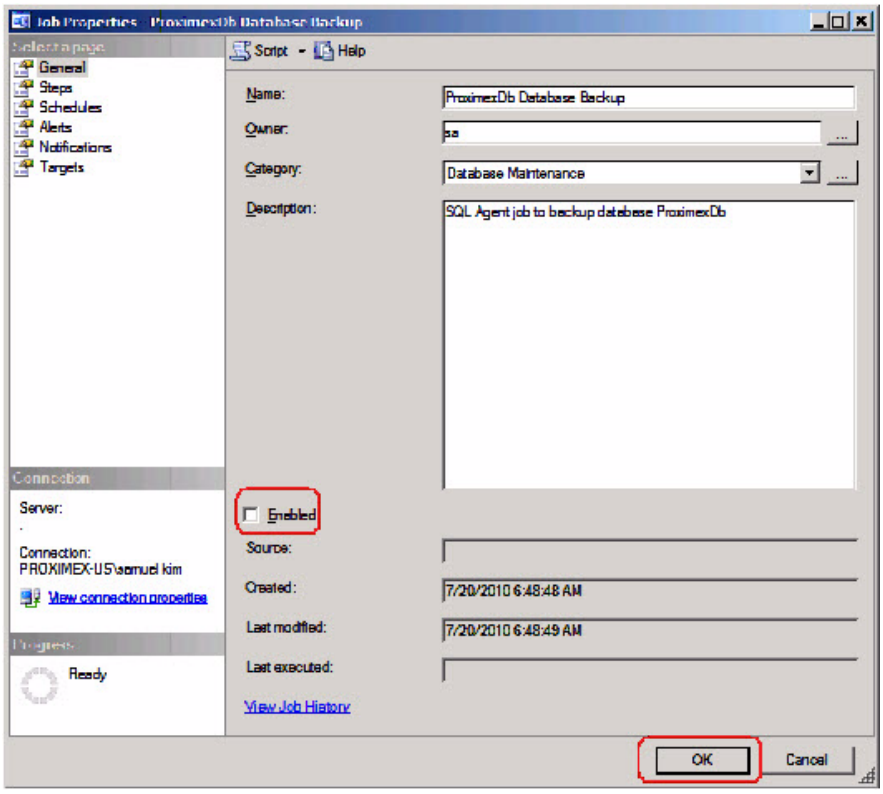


Any existing database backup SQL Server job will fail at this point.

h. To disable database backup jobs for ProximexDb, expand **SQL Server Agent > Jobs** for the Principal SQL Server(.). Right-click **ProximexDB Database Backups** and click **Properties**.

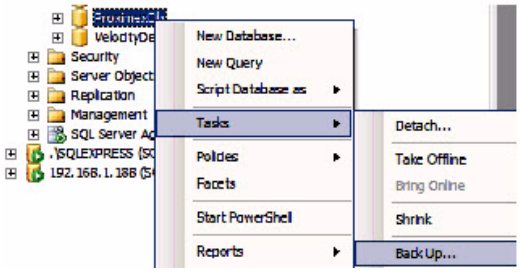


i. In the Job Properties dialog, deselect the **Enabled** option and click **OK**.

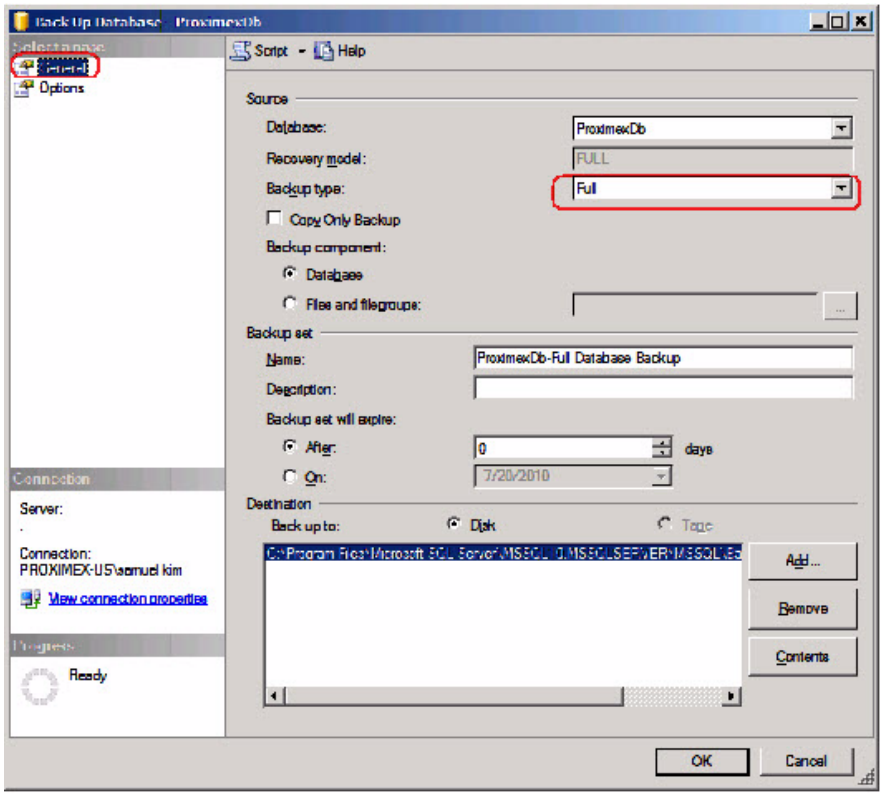


Step 8 Execute a full database backup on the ProximexDb database.

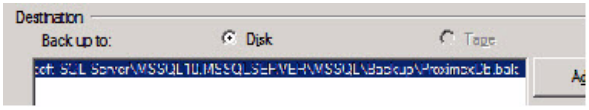
a. Expand the databases under the Principal SQL Server(.). Right-click **ProximexDb** and select **Tasks > Back Up...**.



b. On the **General** tab in the Back Up Database dialog, verify that **Full** is selected from the **Backup type** field.

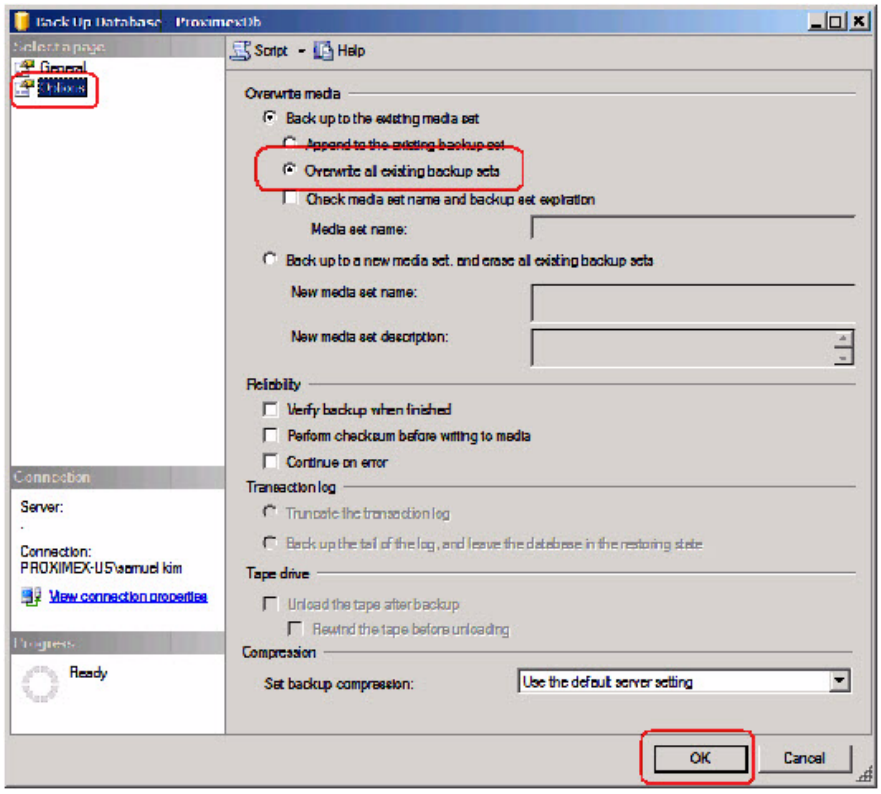


c. Make note of the location specified under Destination.

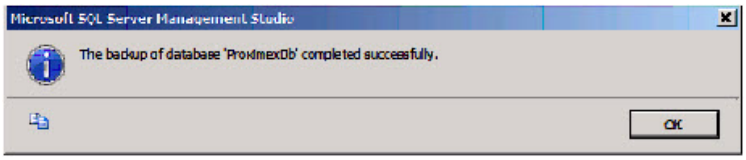


d. Click the **Options** tab.

e. Select **Overwrite all existing backup sets** and click **OK** to start the backup.



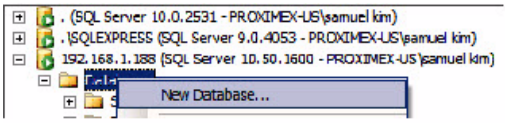
f. A dialog appears to confirm a successful backup. Click **OK**.



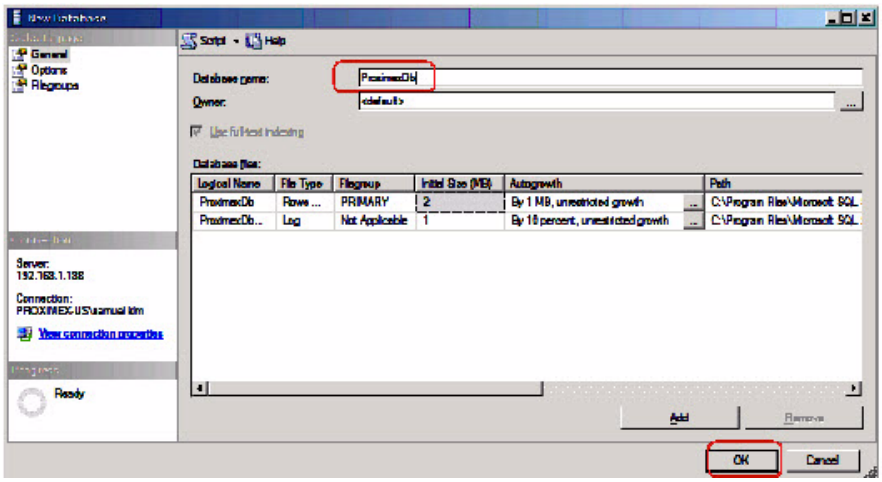
Step 9 Copy the database backup file to the Mirror SQL Server.

Step 10 Create a ProximexDb database on the Mirror SQL Server.

a. Expand the SQL Server database tree for the Mirror SQL Server, right-click **Database** and select **New Database**.



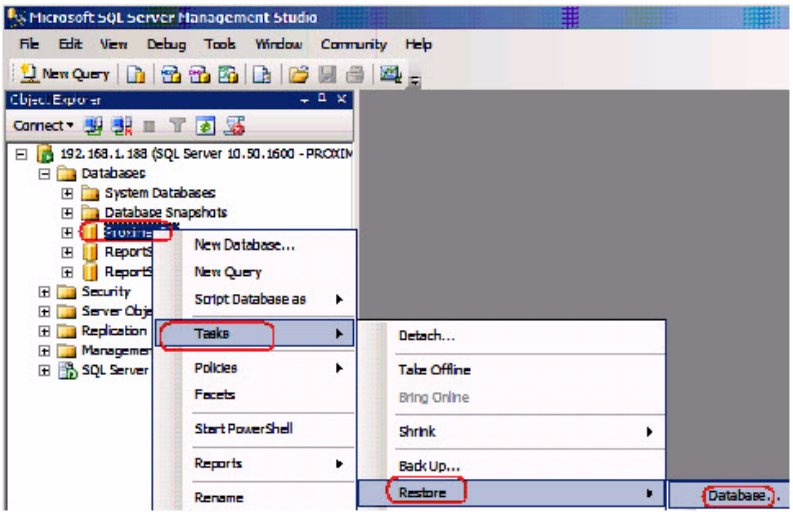
b. In the New Database dialog, enter **ProximexDb** in the **Database name** field. Click **OK** to create the database.



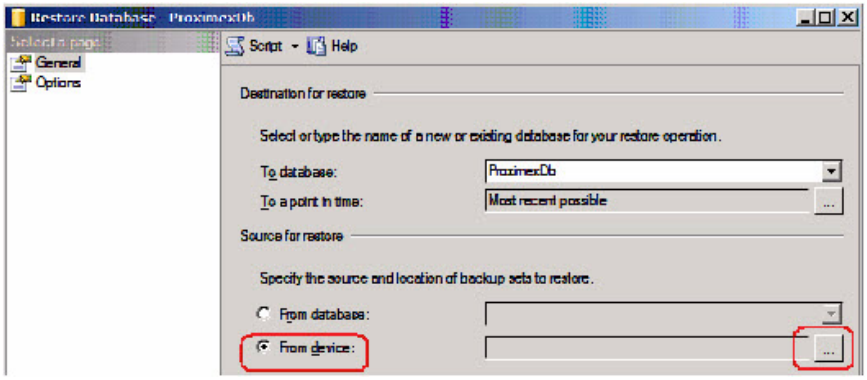
Step 11 Restore the backup ProximexDb database to the Mirror SQL Server with No Recovery mode.

a. Remote login to the machine with the Mirror SQL Server and launch Microsoft SQL Server Management Studio.

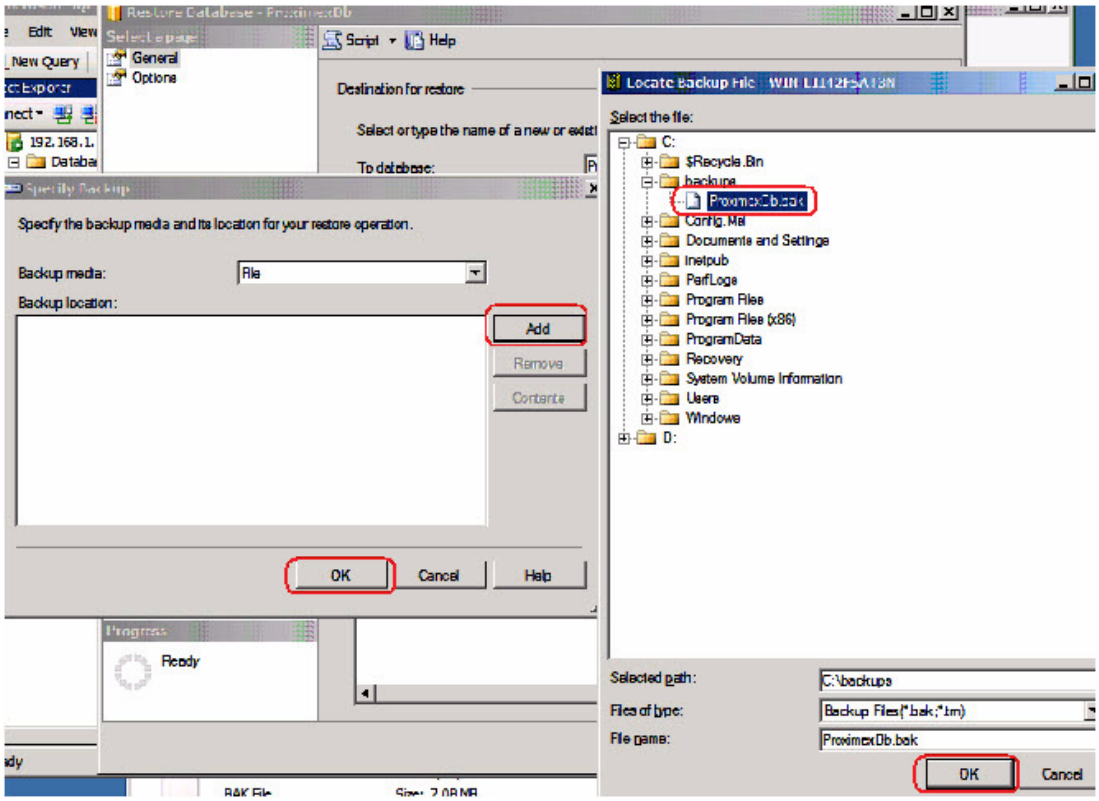
b. Expand the **Databases** under the Mirror SQL Server, right-click **ProximexDb** and select **Tasks > Restore > Database**.



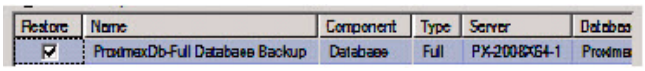
c. In the Restore Database dialog, select **From device** under **Source for restore**, then click **[…]**.



d. In the Specify Backup dialog, click **Add** and navigate to the directory where the backup database file is located. Click **OK**, and **OK** again.



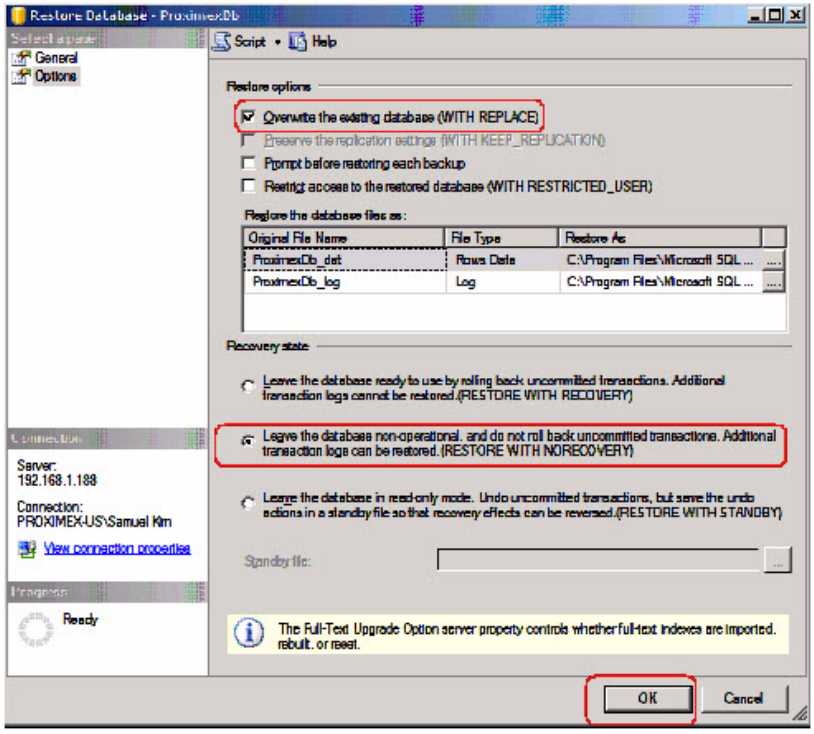
e. Select the **Restore** option in the Restore Database dialog.



f. Click the **Options** tab.

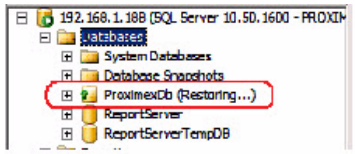
g. Select **Overwrite the existing database**, and **Leave the database non-operational...(RESTORE WITH NO RECOVERY)**.

h. Click **OK** to start the restore process.



i. A dialog appears confirming successful recovery. Click **OK**.

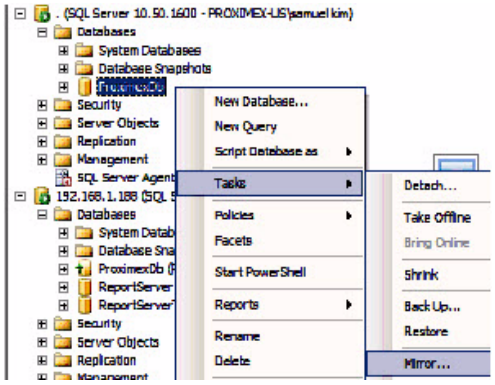
The ProximexDb database should appear in (Restoring…) mode.



Step 12 Activate mirroring of ProximexDb database from the Principal SQL Server.

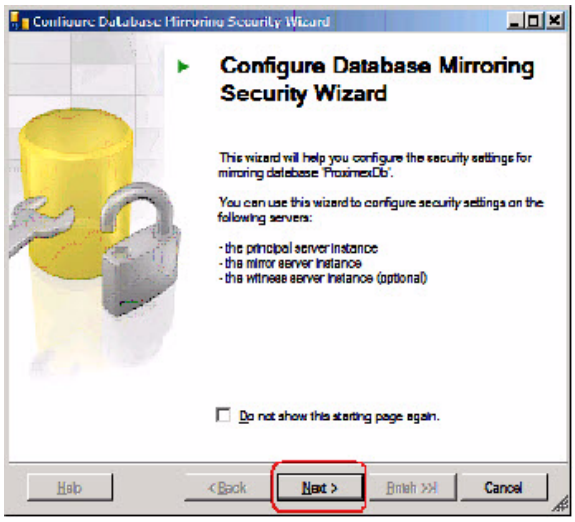
a. Return to Microsoft SQL Server Management Studio on the Principal SQL Server machine.

b. Expand **Databases** under the Principal SQL Server(.), right-click **ProximexDb** and select **Tasks > Mirror…**

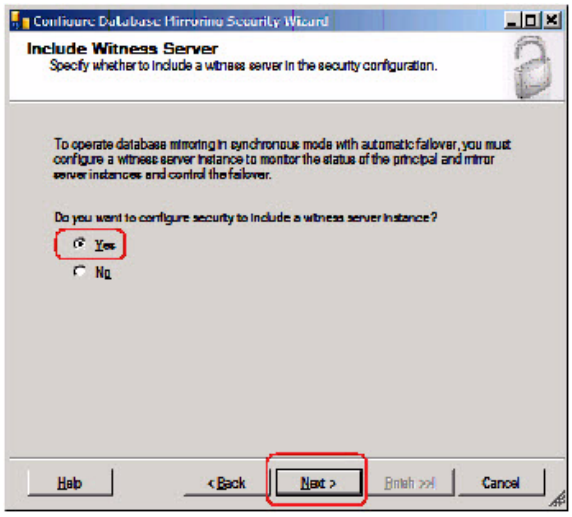


c. On the **Mirroring** tab of the Database Properties dialog, click **Configure Security...**.

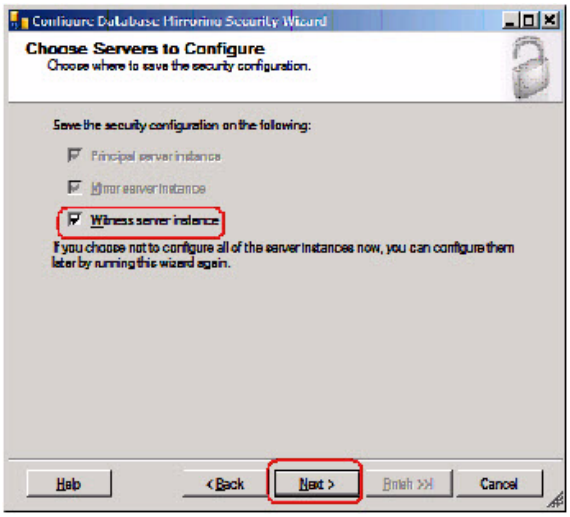
The Configure Database Mirroring Security Wizard appears.



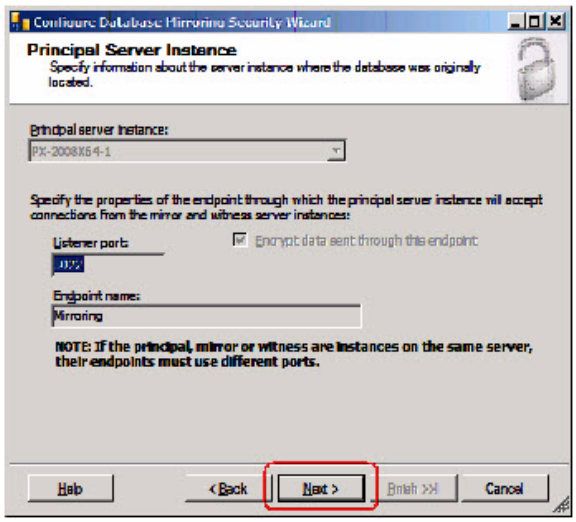
d. Click **Next**.



e. Click **Yes** to include the Witness Server and then click **Next**.

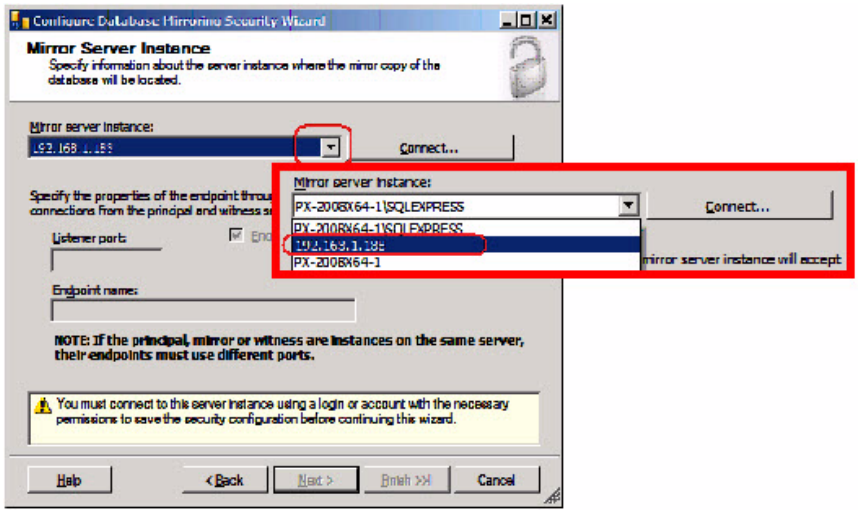


f. Select the **Witness server instance** option to store the configuration on the Witness Server then click **Next**.



As long as SQL Server Management Studio has been launched from the Principal SQL Server and started from ProximexDb, you will not need to configure any information on this screen.

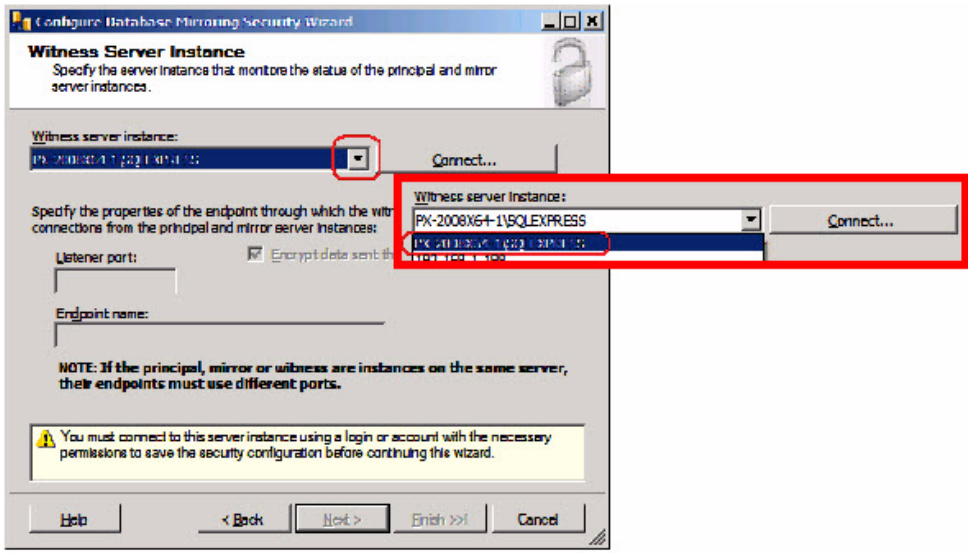
g. Click **Next**.



h. Select the Mirror SQL Server from the **Mirror server instance** field. For this example, it is 192.168.1.188.

i. In the Connect to Server dialog that appears, click **Connect** to establish a connection to the mirrored SQL Server.

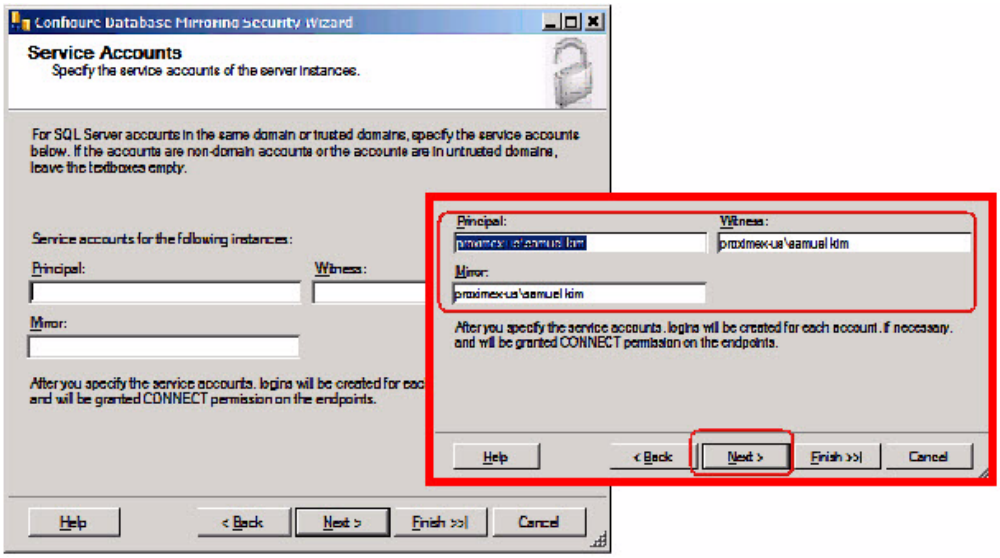
j. After successful connection is established, click **Next** in the Configure Database Mirroring Security Wizard dialog.



k. Select the Witness SQL Server from the **Witness server instance** field. For this example, it is PX-2008X64-1\SQLEXPRESS.

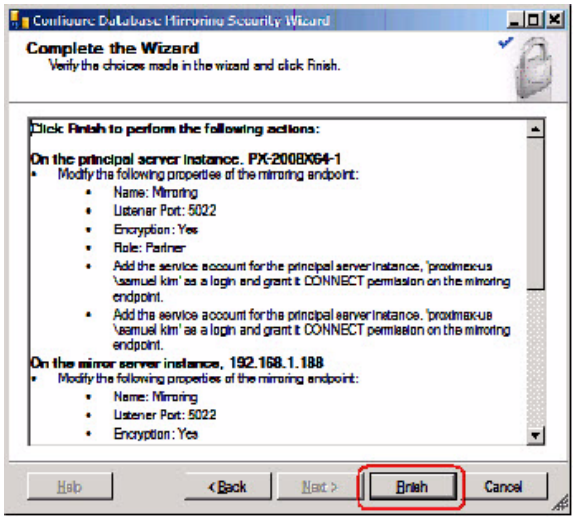
l. In the Connect to Server dialog that appears, click **Connect** to establish a connection to the Witness SQL Server.

m. After successful connection is established, click **Next** in the Configure Database Mirroring Security Wizard dialog.

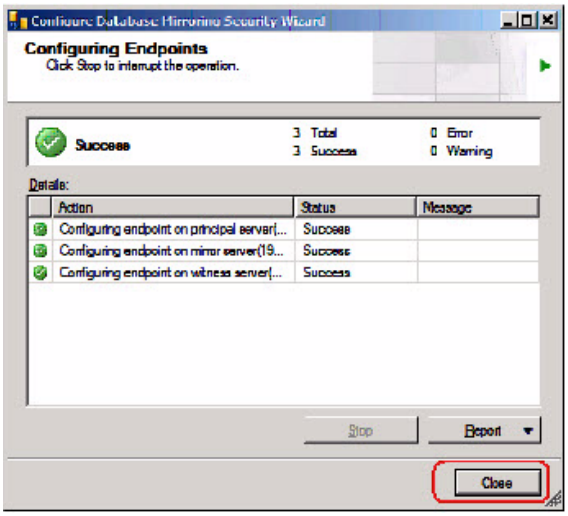


n. Provide service accounts for all three SQL Server instances. It is recommended that you use the same Active Directory user to allow all SQL Server instances to be managed from the same domain account.

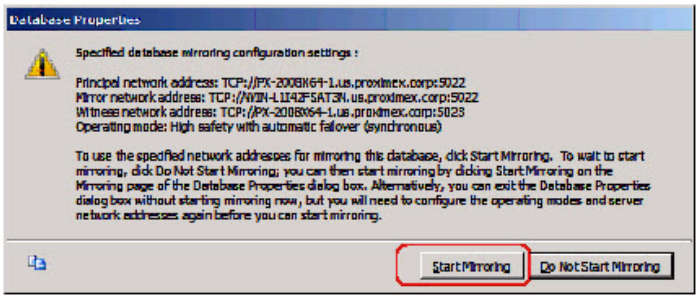
o. Click **Next**. The summary window appears.



p. Click **Finish**.

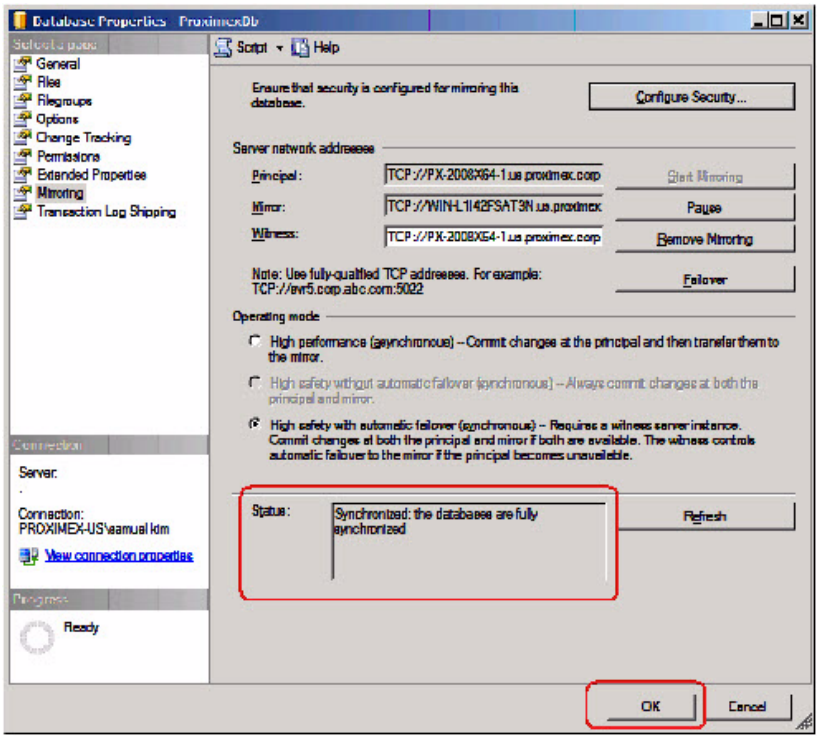


q. Click **Close**. The Database Properties dialog appears.



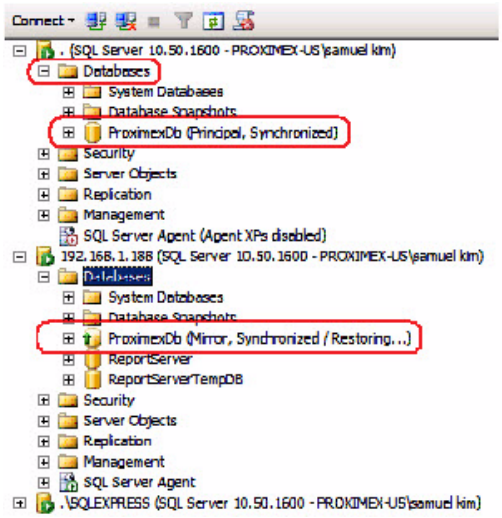
r. Review the result and click **Start Mirroring**.

The Database Properties window reappears. When mirroring is activated the Status area notifies you that the database is fully synchronized.



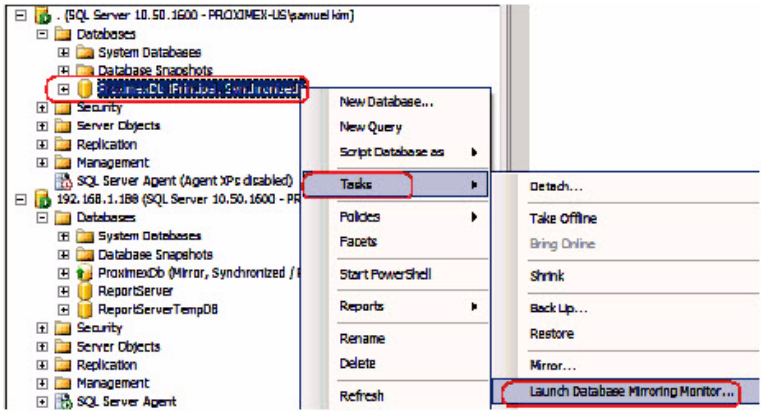
s. Click **OK**.

You can validate that mirroring has been activated by refreshing the Databases node and viewing the results.



Note that the Principal database now appears with (Principal, Synchronized) and the Mirror database now appears with (Mirror, Synchronized / Restoring…).

t. Examine the mirroring monitor by right-clicking **ProximexDb** and selecting **Tasks > Launch Database Monitoring Monitor…**



The Database Mirroring Monitor window shows performance information about the mirroring process.

Click **History [...]** to view historic information about the mirroring process.

Initiating Manual Failover

You can manually failover to the Mirror SQL Server in several ways. This section describes how to failover from the Mirroring tab in the Database Properties dialog.

To manually failover, follow these steps:

Procedure

Step 1 Launch SQL Server Management Studio on the Principal SQL Server machine.

Step 2 Expand the **Databases** for the Principal SQL Server, right-click **ProximexDb** and select **Tasks > Mirror...**.

Step 3 Click **Failover** to initiate a manual failover.

Step 4 Click **Yes** in the Database Properties dialog that appears.

After refreshing the Databases node, you will see that the Mirror SQL Server and Principal SQL Server have now switched roles.

Setting up PSOM Web Service for Database Mirroring

To configure PSOM Web Service for database mirroring, follow these steps:

Procedure

Step 1 Complete the steps in the "Mirroring PSOM Repository" section on page E-3.

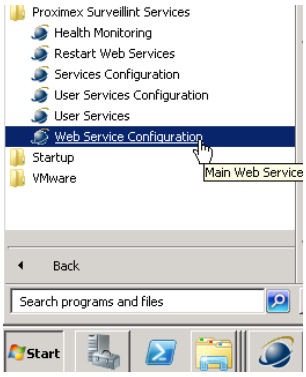
Step 2 Start the PSOM Web Service (if not already started).

Step 3 Open the **Service Manager** by clicking **Start > Administrative Tools > Services**, and verify that the following services are running: PSOM Bus Services, PSOM Business Logic Core Services, PSOM Caching Services, PSOM Monitoring Logic Services, PSOM Collaboration Services, PSOM Health Monitoring Services, and PSOM Sensor Management Services.

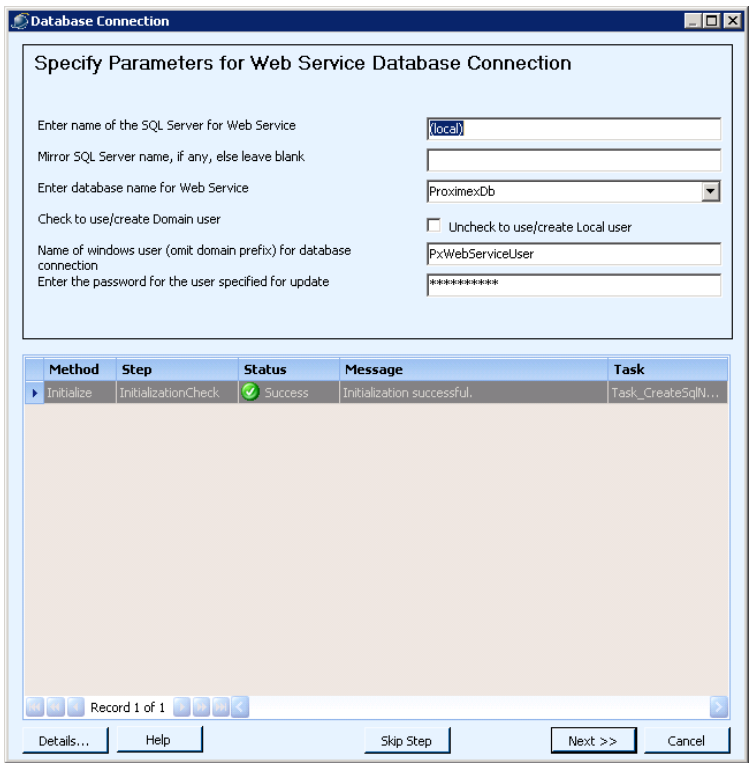
Step 4 Failover to the Mirror SQL Server following the steps in the "Initiating Manual Failover" section on page E-21.

Step 5 With the Mirror SQL Server acting as the Principal SQL Server:

a. Select **Start > All Programs > Cisco Physical Security Operations Manager 6.1 Services > Web Service Configuration**.



The Database Connection window appears.



b. Enter the Mirror SQL Server in the **Enter the name of SQL Server for Web Service** field.

c. Leave the **Mirror SQL Server name** field blank.

d. Select **ProximexDb** from the **Enter database name for Web Service**.

e. Select the **Check to use/create Domain user** option since the account for the SQL connection must be a domain account. The necessary local account for database connectivity will be created.

The PSOM Web Service is now configured to communicate with the Mirror SQL Server.

f. Validate that the PSOM Web Service can connect with the Mirror SQL Server by launching the Administration Console and logging in. Close the Administration Console after logging in.

Step 6 Failover to the Principal SQL Server following the steps in the "Initiating Manual Failover" section on page E-21.

Step 7 With the Principal SQL Server in control, repeat Step 5 except:

- Enter the Principal SQL Server in the **Enter the name of SQL Server for Web Service** field.
- Enter the Mirror SQL Server in the **Mirror SQL Server name** field.

Setting up PSOM Services for Database Mirroring

To configure PSOM Services for database mirroring, follow these steps:

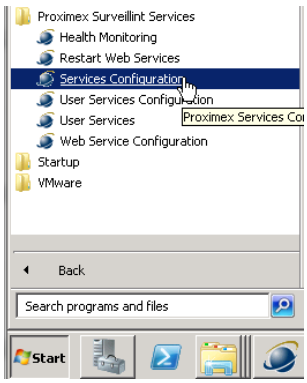
Procedure

Step 1 Complete the steps in the "Mirroring PSOM Repository" section on page E-3.

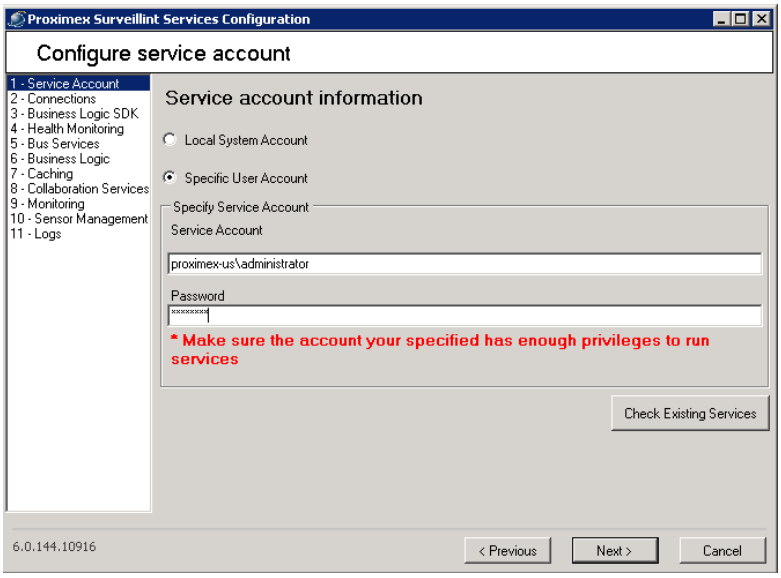
Step 2 Complete the steps in the "Setting up PSOM Web Service for Database Mirroring" section on page E-21.

Step 3 Start the PSOM Web Service (if not already started).

Step 4 Select **Start > All Programs > Cisco Physical Security Operations Manager 6.1 Services > Services Configuration**.

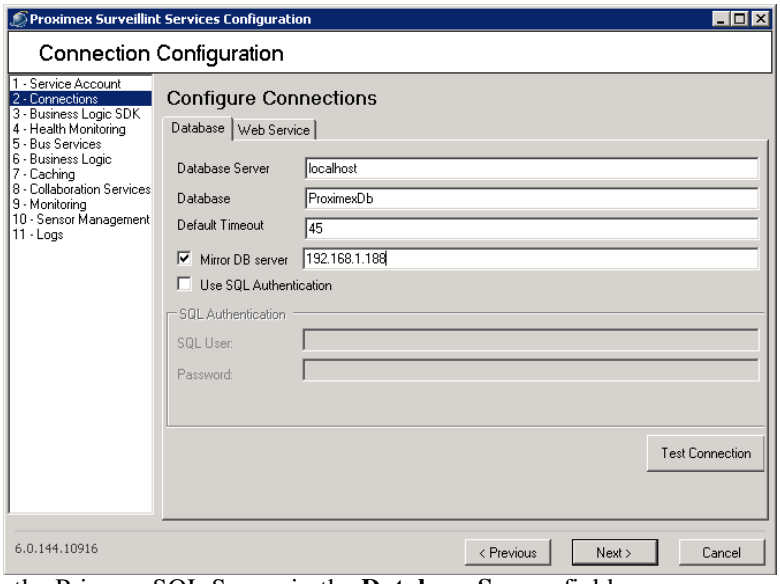


The Services Configuration window appears.



Step 5 Select **Specific User Account** and provide the domain account and password that has been designated to access SQL Server and each of the databases.

Step 6 Click **2 – Connections**.



Step 7 Enter the Primary SQL Server in the **Database Server** field.

Step 8 Select the **Mirror DB Server** option and enter the Mirror SQL Server in the field.

Step 9 Click **11 – Logs**.

Step 10 Click **Finish**.

INDEX