



## **Cisco Prime Service Catalog 12.1 Installation and Upgrade Guide**

31 August, 2017

**Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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 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](http://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. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

*Cisco Prime Service Catalog 12.1 Installation and Upgrade Guide*  
© 2017 Cisco Systems, Inc. All rights reserved.



---

**CHAPTER 1**

<b>Installation Overview</b>	<b>1-1</b>
Deployment Topology	1-1
High-level Installation Flow	1-5
High-level Installation Overview	1-6

---

**CHAPTER 2**

<b>Installation Requirements</b>	<b>2-1</b>
About Prime Service Catalog Licensing	2-1
Software Requirements	2-1
Software Configuration Prerequisites	2-2
Browser	2-2
Application Server	2-3
Web Server	2-3
Internet Information Service (IIS) with WildFly	2-3
Java Development Kit	2-4
Database	2-4
LDAP	2-5
IBM Cognos	2-5
Other Miscellaneous Settings	2-5
Hardware Requirements	2-6
Sizing	2-6
Minimum Hardware Requirements for Application Server Host	2-6
Minimum Hardware Requirements for Web Server Host	2-6
Minimum Hardware Requirements for Database Host	2-7
Minimum Hardware Requirements for Reporting Server Host	2-7

---

**CHAPTER 3**

<b>Configuring the Service Catalog Database</b>	<b>3-1</b>
Configuring Oracle	3-1
Oracle Parameters	3-1
catcio.sql Package	3-2
Redo Logs	3-2
Unicode Character Set	3-2
Creating Tablespaces and Database Schema for Hosting Service Catalog Data	3-2
Configuring Oracle RAC 12C	3-4

- Configuring Microsoft SQL Server 3-4
  - Default Instance or Named Instance 3-4
  - Mixed-Mode Authentication 3-4
  - Creating ServiceCatalog Database and Login User 3-4
  - Adding -T272 Property to SQL Server Database 3-5
  - Setting Compatibility Mode 3-6

**CHAPTER 4**

**Setting Up WildFly Application Server 4-1**

- Preinstallation Tasks for WildFly 4-1
  - Preinstallation Checklist 4-2
  - WildFly Installation Flow 4-3
  - Installing Java 4-4
    - Oracle JDK 4-4
    - Red Hat OpenJDK 4-4
  - Preparing IIS Web Server 4-5
  - Downloading Prime Service Catalog Software Image 4-5
- Installing Prime Service Catalog on WildFly Application Server 4-6
  - Setting Up WildFly Standalone Application Server 4-6
    - Performing a Standalone Installation For WildFly Application Server 4-7
  - Setting Up WildFly Clustered Application Servers 4-10
    - Performing WildFly Cluster Installation for Two VM Topology 4-11
    - Performing WildFly Cluster Installation for Four VM Topology 4-18
- Postinstallation Tasks for WildFly 4-28
  - Postinstallation Tasks for WildFly Standalone Application Server 4-28
    - Enabling Secure Cookie 4-28
    - Starting WildFly Server on Linux 4-29
    - Starting WildFly Server on Windows 4-29
    - Configure WildFly as Windows Service 4-30
  - Postinstallation Tasks for WildFly Clustered Application Servers 4-30
    - Configure WildFly as Windows Service 4-31
    - Setting Up Apache Web Server on WildFly 4-31
    - Enabling SSL on Apache Web Server and IIS Server 4-34
    - Applying Patch or Customizations to the WildFly Cluster Setup 4-35
- Verifying Your Installation 4-39

**CHAPTER 5**

**Setting Up WebLogic Application Server 5-1**

- Preinstallation Configuration for WebLogic 5-1
  - WebLogic Installation Flow 5-2
  - Installing Java 5-3

Downloading Prime Service Catalog Software	5-3
Installing Custom Java Libraries	5-3
Creating a Managed WebLogic Server	5-4
Setting the Arguments for Java Virtual Machine	5-7
WebLogic Cluster Configuration	5-8
Configuring JMS Server	5-9
Creating a Persistent Store	5-9
Creating a JMS Server	5-9
Creating a JMS Module	5-10
Creating Connection Factory	5-10
Creating JMS Templates	5-11
Creating Queues	5-11
Configuring JDBC Data Sources	5-12
Configuring Basic Authentication for NSAPIs	5-15
Restarting WebLogic Server	5-15
Installing Prime Service Catalog on WebLogic Application Server	5-17
Performing a Typical Installation	5-17
Before You Begin	5-17
Procedure	5-18
Performing a Custom Installation	5-20
Before You Begin	5-20
Procedure	5-20
Postinstallation Configuration for WebLogic	5-23
Extracting WAR Files	5-23
Deploying the WAR Files to Managed Server	5-24
Extracting and Deploying wls-management-services.war	5-24
Deploying ISEE.war	5-24
Deploying RequestCenter.war	5-25
Verifying Your Installation	5-26
Redeploying a Server	5-26
Configuring Web Server	5-27

**CHAPTER 6****Upgrading Prime Service Catalog** 6-1

Overview	6-1
Release Upgrade Path	6-1
Limitations and Notes	6-1
What is Upgraded	6-3
What is Not Upgraded	6-3
Assumptions and Best Practices	6-4

- Prerequisites 6-4
- High-Level Upgrade Procedure 6-4
- Upgrading Prime Service Catalog 6-6
  - Performing Preupgrade Tasks 6-6
    - Migrating the Audit Log Data 6-7
  - Preparing the Upgrade Environment 6-8
  - Run the Installation Wizard to the Validation Page 6-9
  - Validating Database 6-10
  - Validating Schema 6-14
  - Validating Data 6-14
  - Repairing the Database 6-15
  - Completing Installation 6-15
  - Performing Post-upgrade Tasks 6-16
  - Moving Customizations to Website 6-17
    - High-Level Steps to Migrate to Website Model: 6-17
    - Working of Script GenerateCSV.py 6-17
    - Working of Script ChangePathReferences.py 6-18

**CHAPTER 7**

**Installing and Upgrading Reporting Module 7-1**

- Prerequisites for Installing Reporting 7-1
  - Cognos Application Server Requirements 7-1
    - Operating Systems 7-1
    - Memory and Disk Space 7-1
    - Internet Information Services (IIS) 7-2
    - Internet Explorer 7-2
    - Database Client Connectivity 7-3
    - Other Requirements 7-3
  - Cognos Database Server Requirements 7-4
    - Creating Data Mart and Content Store Databases for Oracle 7-4
    - Creating Data Mart and Content Store Databases for MS SQL Server 7-6
    - Sizing the Content Store Database 7-6
  - Installing Cognos Software 7-7
    - Downloading Cognos Software 7-7
    - Installing Cognos Business Intelligence Server 7-8
    - Installing Cognos Data Manager 7-8
    - Installing Cognos Fix Pack 7-9
- Installing Reporting 7-10
  - Executing Reporting Setup 7-10
  - How to Use the Installation Wizard 7-11

Running the Reporting Installation Wizard	7-11
Executing create_datasource.cmd	7-20
Importing Service Catalog Reports	7-21
Restart the Service Catalog Application	7-22
Configuring Advanced Reporting	7-22
Postinstallation Tasks	7-23
Postinstallation Tasks for Reporting	7-23
Postinstallation Tasks for Advanced Reporting	7-24
Using Reporting Module with Oracle RAC Database	7-24
Upgrading Reporting	7-25
Performing Preupgrade Tasks for Reporting	7-25
Backing Up Data Mart and Content Store Artifacts	7-25
Uninstalling Cognos 8.4.x Components	7-25
Installing Cognos 10.2.1 Software	7-26
Running the Reporting Installer for Upgrade	7-26
Performing Post-upgrade Tasks for Advanced Reporting	7-26
Migrating Custom Reports	7-26
Reporting Upgrade Issue and its Workaround	7-27
Uninstalling Reporting	7-28

**APPENDIX A****Worksheets A-1**

Database Information Worksheet	A-1
WildFly Application Server Information Worksheet	A-2
WebLogic Application Server Information Worksheet	A-3
Supported Time Zone	A-5
Reference Tables for Installation Procedures	A-7

**APPENDIX B****WildFly Scripts B-1**

Scripts for WildFly Standalone Application Server	B-1
Scripts for WildFly Cluster Application Server	B-1
Adding Subsequent Host Nodes Manually in WildFly Cluster	B-5
Configuring Plugin for IIS Web Server	B-7
Add Web Server Role for IIS	B-7
Install Tomcat Plugin	B-8
Copy WAR Directories	B-8
Create Virtual Directories for IIS	B-9
Modify Plugin Properties	B-10
Configure Instance-ID for WildFly	B-12

For 4 VM Topology **B-12**  
For 2 VM Topology **B-14**  
Test IIS **B-16**  
Configuring Data Source for SQL in WildFly **B-17**  
Configuring Data Source for Oracle in WildFly **B-18**

---

**APPENDIX C**

**Port Usage for Prime Service Catalog C-1**





# Installation Overview

---

This guide describes the installation process using standalone installer. Cisco Prime Service Catalog comprises of two required component applications, Service Catalog and Service Link, and one optional component application called Reporting.

The installation is supported on WildFly and WebLogic application servers and can be configured in either Standalone and Cluster setup.

Subsequent sections in this chapter describes various deployment topologies for both WildFly and WebLogic Application Servers.

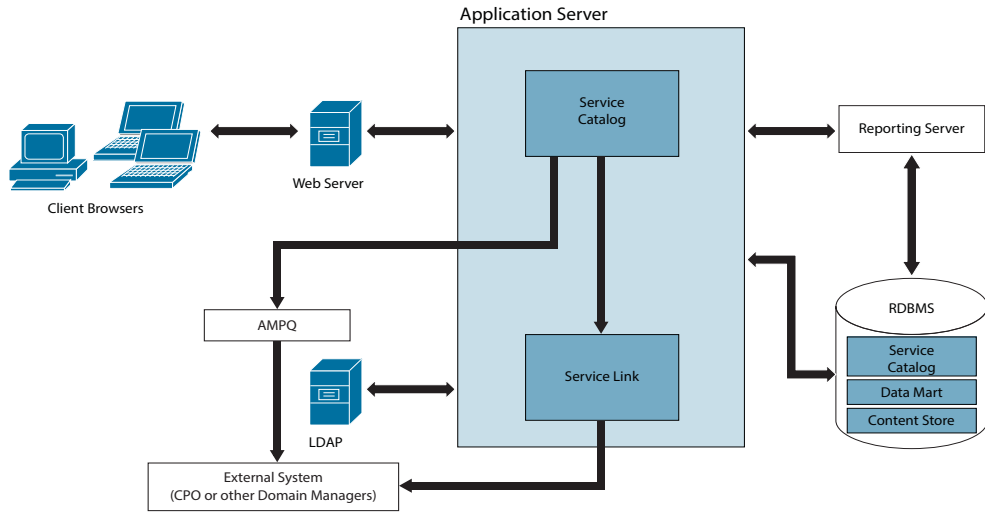
For information about installing the 12.1 Virtual Appliance (OVA file), see [Cisco Prime Service Catalog Quick Start Guide](#).

## Deployment Topology

Prime Service Catalog can be set up in a standalone or cluster mode.

- **Standalone Mode:** In WildFly or Weblogic standalone mode, Prime Service Catalog provides two types of installation —Typical and Custom. The Typical installation performs a streamlined installation using default settings. Using the custom option, you can choose to install only the Service Catalog component application on your computer, only the Service Link component application on your computer, or both Service Catalog and Service Link component applications together on the same computer.

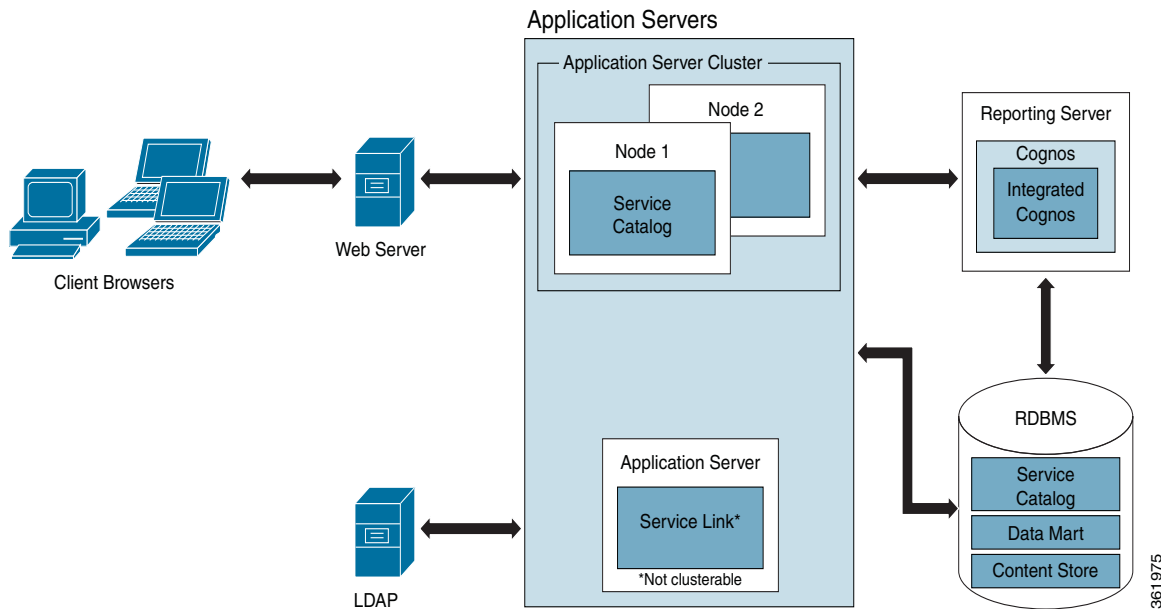
Figure 1-1 Typical Topology



• Cluster Mode:

- For a WebLogic Cluster environment, the topology may include multiple application server machines. The following diagram shows an example of an application server cluster with two nodes containing the Service Catalog component application, and a standalone application server containing the Service Link component application:

Figure 1-2 Clustered Topology

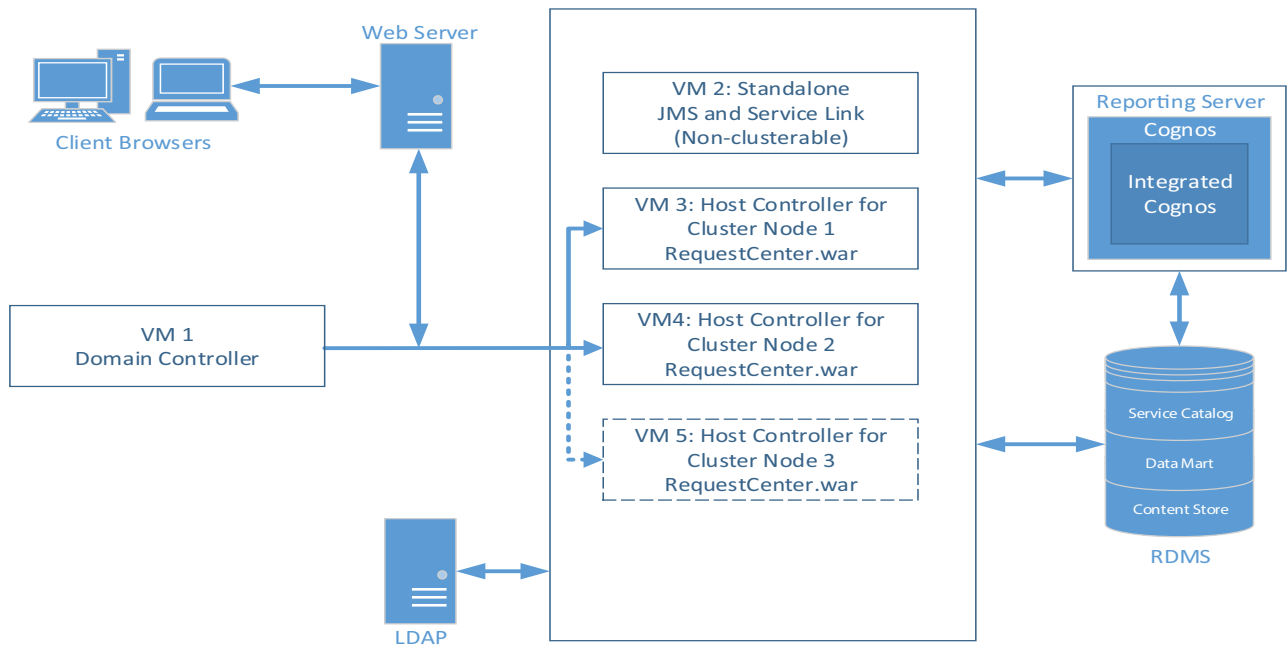


- For WildFly Cluster environment, the available topologies are a two VM and a four VM topology.

The following diagram shows an example of a four VM topology that has an application server cluster with two nodes containing the Service Catalog component application, one with domain controller and another node with Service Link component application.

- VM 1 will have only the Domain Controller.
- VM 2 will have the Service Link and JMS server.
- VM 3 will be the Host 1 for Service Catalog.
- VM 4 will be the Host 2 for Service Catalog.

**Figure 1-3 WildFly 4 VM Topology**



The following diagram shows an example of a two VM topology that has two horizontal nodes (i.e. two separate hosts) in a Wildfly cluster configuration. One node contains the Service Catalog component application, and another contains a Domain Controller, Service Link component application, and Service Catalog component application.

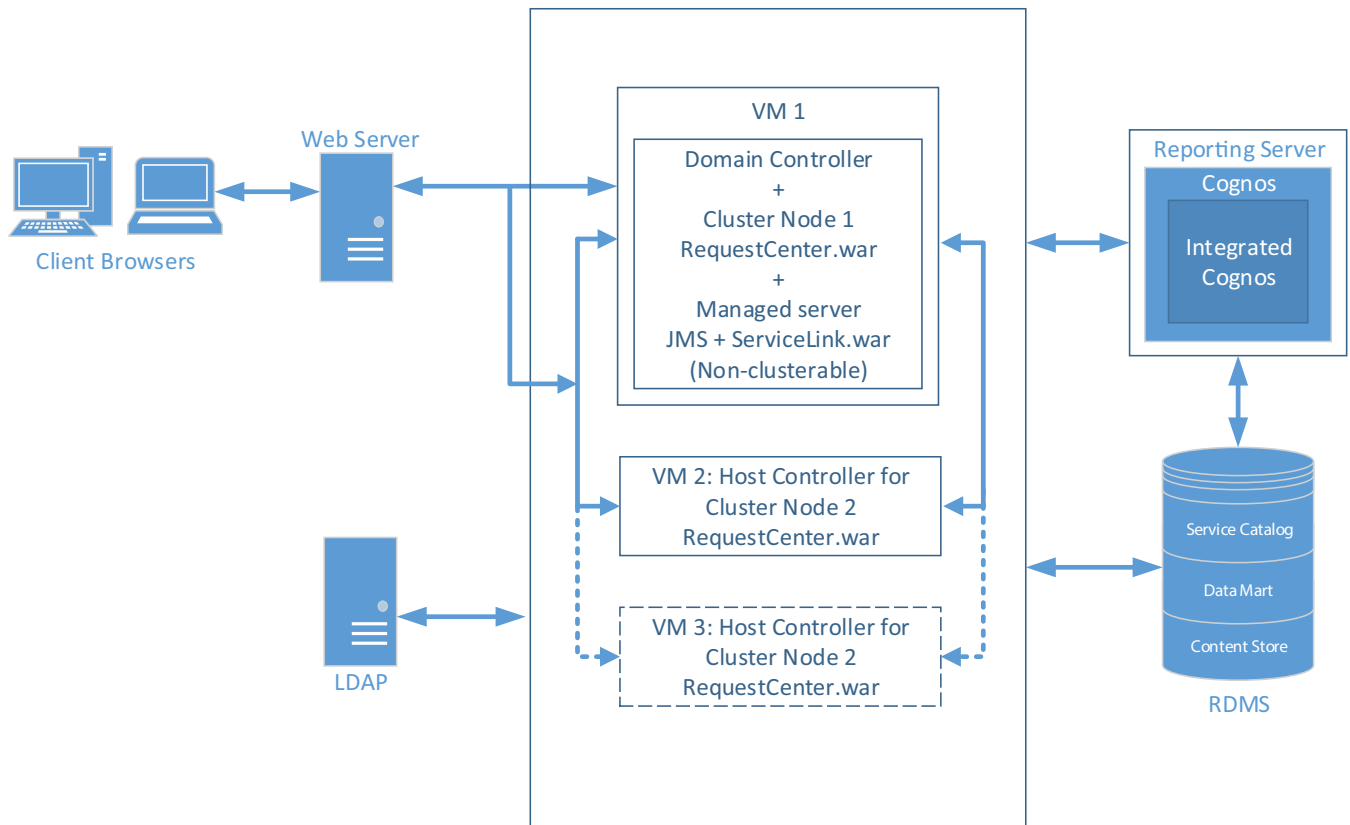
The user can start with 2 nodes, and add more nodes (i.e. more hosts) to the cluster as desired.



**Note**

The Prime Service Catalog Installer will support up to 6th node for the cluster. If the user wants to add a 7th node or more, see section [Adding Subsequent Host Nodes Manually in WildFly Cluster](#).

Figure 1-4 WildFly 2 VM Topology



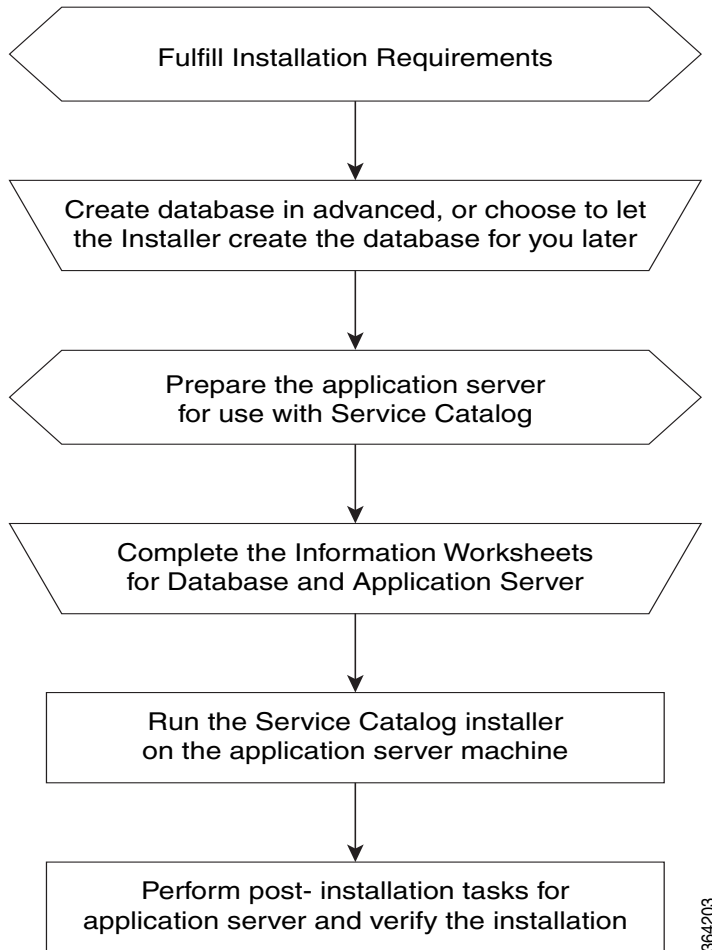
406036

Next chapter describes the software and hardware requirements for a typical deployment topology.

# High-level Installation Flow

The following flowchart provides a high level flow of Prime Service Catalog installation.

**Figure 1-5** Common Installation Steps



# High-level Installation Overview

This section provides a road map of the installation process for Prime Service Catalog:

- 
- Step 1** Follow the instructions provided in [Installation Requirements](#) to ensure that you have adequately addressed the minimum hardware and software requirements, and installed the prerequisite software.
  - Step 2** Create the Service Catalog database, as described in [Configuring the Service Catalog Database](#) and complete the [Database Information Worksheet](#). You will need this information when running the Prime Service Catalog installation wizard.
  - Step 3** Prepare the application server for use with Prime Service Catalog, by performing the tasks described in one of the following sections:
    - For WildFly, go to the [Preinstallation Tasks for WildFly](#).
    - For WebLogic, go to the [Preinstallation Configuration for WebLogic](#).Complete the respective Application Server Information Worksheet as described in the [Worksheets](#) section. You will need this information when running the Prime Service Catalog installation wizard.
  - Step 4** Run the Prime Service Catalog installer on the application server machine, as described in the [Installing Prime Service Catalog on WildFly Application Server](#) or [Installing Prime Service Catalog on WebLogic Application Server](#). If you are performing an upgrade installation from a previous release, see [Upgrading Prime Service Catalog](#) in conjunction with this section.
  - Step 5** Perform the post installation tasks for your application server and verify your installation as described in one of the following sections:
    - For WildFly, go to the [Postinstallation Tasks for WildFly](#).
    - For WebLogic, go to the [Postinstallation Configuration for WebLogic](#).
  - Step 6** To enable the Reporting features, you also need to install the Reporting software module and the Cognos software, and configure the Cognos Server to integrate with the Prime Service Catalog application. When you are ready to do this, follow the instructions in [Installing and Upgrading Reporting Module](#).
-



# Installation Requirements

Before installing Prime Service Catalog, review the licensing and the installation requirements described in this chapter.

## About Prime Service Catalog Licensing

Cisco ONE Enterprise Cloud Suite is a part of the Cisco ONE for Data Center solution and consists of four components: Infrastructure Automation, Cloud Management, Big Data Automation and Service Management. Each component can be used individually, or all components can be used together to create an integrated hybrid cloud solution. All components were designed to work together, providing you with an incremental approach to hybrid cloud automation.

The Cisco ONE ECS Service Management package which includes Cisco Prime Service catalog and Cisco Process Orchestrator is sold as a one-year, three-year, or five-year subscription and a customer can order the Service Management Base bundle with an option to add-on the Service Management

For more information about licensing contact your account manager.

## Software Requirements

The following table lists the supported third-party software for this release of Cisco Prime Service Catalog. Also refer to the “Cisco Prime Service Catalog Compatibility Matrix” document.

**Table 2-1 Supported Software**

<b>Browser</b>
Internet Explorer 11
Mozilla Firefox ESR 49.0.2 (or later ESR)
Chrome 54 (or later)-(supported for the following modules only: Service Catalog, Order Management, My Services, Service Portal, Demand Management, Service Manager, Tenant Management)
Safari 10.0.x(on MAC OS only) (supported for the following modules only: Service Catalog, Order Management, My Services, Service Portal, Demand Management, Service Manager, Tenant Management)
<b>Browser Plugin</b>

**Table 2-1 Supported Software (continued)**

The graph on the Service Link Home Page is optional and for informational purpose only. Adobe® Flash® Player is required to display the graph on the Service Link Home Page.

**Web Server**

Apache Http Server 2.4.6 or RedHat Http Server 2.4.6

Microsoft Internet Information Services (IIS) 8.5

**Application Server + Java Development Kit**

WildFly 10.1.Final + Oracle JDK 8 Update 131 (or higher Update) + JCE Unlimited Strength Policy Jars (on Windows Server)

Oracle WebLogic 12c (12.2.1.2) + Oracle Hotspot JDK 8 Update 91 (or higher Update) + JCE Unlimited Strength Policy Jars

WildFly 10.1.Final + Red Hat OpenJDK 1.8.0\_131 (or higher 1.8.0\_x) (on Red Hat Enterprise Linux)

**Application Server Operating System**

Red Hat Enterprise Linux Server 7.3 (64 bit)

Microsoft Windows Server 2012 R2 (64 bit)

**Database**

Oracle 12c, version 12.1.0.2  
(Express Edition of Oracle Database is not supported)

Microsoft SQL Server 2012 and 2016  
(Express Edition of SQL Server is not supported)

**LDAP**

Microsoft Active Directory Server 2012

**IBM Cognos®**

(Note: IBM Cognos software is only supported on Microsoft Windows Server 2012 R2 64-bit Operating System.)

IBM Cognos Business Intelligence Server, version 10.2.1, plus Fix Pack 2

IBM Cognos Data Manager, version 10.2.1, plus Fix Pack 2

## Software Configuration Prerequisites

This section describes how to configure the software listed above for use with Prime Service Catalog.

### Browser

The following settings must be configured on the web browser used to connect to the Prime Service Catalog application:

- Popup blocker is turned OFF.
- Cookies are enabled.
- Adobe Reader® is required on your web browser machine, if you plan to view and print reports.



## Application Server

If you choose Wildfly as your application server, you do not need to install Wildfly software as a prerequisite. The Cisco Prime Service Catalog installer will automatically install the Wildfly Application Server and deploy the Service Catalog applications. Follow the instructions in the [Preinstallation Tasks for WildFly](#) to prepare your machine for installing Prime Service Catalog with the Wildfly Application Server.

If you choose WebLogic as your application server, you need to install the Oracle WebLogic Application Server software as a prerequisite on your machine. This guide does not contain instructions for installing the WebLogic software. However you will need to follow the instructions in the [Preinstallation Configuration for WebLogic](#) to prepare your WebLogic Server for use with Prime Service Catalog.

## Clustering Considerations

To deploy Prime Service Catalog in a clustered environment, WildFly and WebLogic Application Server must be set up in a clustered configuration before you install Prime Service Catalog. Additionally, if you want to provide full fail-over capability, then you must configure cluster-able sessions on one or more of the clustered nodes. See your application server documentation for information on clustered configuration.

## Web Server

As a prerequisite, your web server must already be installed and running. Your web server does not have to be installed on the same machine as your application server, or on the machine where you plan to execute the Service Catalog installer.

The web server must have the plugin configuration necessary to communicate with your application server. For example, if you choose to use Apache web server with WebLogic Application Server for your deployment topology, then as a prerequisite, you need to manually configure the plugin for your Apache server to connect to your WebLogic server. The plugin between the web server and the application server will not be configured by the Service Catalog installer.

To ensure that the web server (in this case, Apache) does not disclose the web server type, version, and other vulnerable information, you must configure Apache to provide custom error responses.

For details, see:

<http://httpd.apache.org/docs/current/custom-error.html>

## Internet Information Service (IIS) with WildFly

If you select Wildfly as your application server on a Windows Operating System, the Service Catalog installer can configure the Tomcat plugin for the IIS web server automatically for you, if it detects that the IIS web server is already installed on the same Windows machine where you execute the installer.

You will see the "Configure IIS" option on the installation wizard during the installation for both Service Catalog and Service Link. You can select or deselect that option as you desire. To enable this feature, the IIS web server must meet the following required settings:

- IIS Web Server is installed on the same Windows machine where you execute the Service Catalog installer
- IIS Web Server has the following Role Services: ISAPI Filters, ISAPI Extensions
- IIS must be stopped prior to executing the Prime Service Catalog installer
- You can use a customized website. To add a customized website, first add the customized website in the Internet Information Services (IIS) Manager and bind them to appropriate port, for example: Port 88, 90.

**Note**

After you install Prime Service Catalog for Wildfly, refer to the section [Configuring Plugin for IIS Web Server](#) for additional instructions on how to configure IIS Plugin.

## Java Development Kit

Java Development Kit is a prerequisite software on your application server machine. As listed in [Table 2-1](#), only specific versions (and vendors) of JDK are supported for each type of application server. More information about how to configure Java for your application server is described in the [Preinstallation Tasks for WildFly](#), or the [Preinstallation Configuration for WebLogic](#).

Java 1.8 is also a prerequisite for the Cisco Prime Service Catalog installer. Therefore, if you plan to execute the Service Catalog installer on a machine different from your application server, then you need to install Oracle Java or OpenJDK on that machine. If you plan to execute the Service Catalog installer on the same machine where your application server is installed, then just set JAVA\_HOME environment variable to the same Java that is used by your application server.

Prime Service Catalog supports AES algorithm and 256 bit symmetric keys. Therefore, if you use Oracle Java, you must also install the "JCE Unlimited Strength Crypto Policy" jar files on the JAVA\_HOME directory to enable 2048 bit encryption. If you do not install JCE Unlimited Strength Crypto Policy for Oracle Java, the Application Server displays an error message and aborts the installation. For instructions on how to install the JCE Unlimited Strength Policy jar files, see the [Oracle Website](#).

**Note**

Red Hat OpenJDK already comes with unlimited strength policy so you don't need to install any additional jar files for OpenJDK.

## Database

If you choose Oracle 12c as your RDBMS, you need to install the Oracle 12c Database Server software as a prerequisite (see [Table 2-1](#) for specific version).

For database connection failover scenarios, you can use Oracle RAC 12C for your databases. For more information on configuring Oracle RAC 12C, see [Configuring Oracle RAC 12C](#).

If you choose SQL Server 2012 or 2016 as your RDBMS, then you need to install the respective Microsoft SQL Server software as a prerequisite (see [Table 2-1](#) for specific version).

Do not install any SQL Server Client or Oracle Client connectivity software on your application server. You must use the JDBC driver that is bundled with the Cisco Prime Service Catalog product. For the WildFly application server, the Cisco Prime Service Catalog installer automatically installs the appropriate JDBC driver and configures the JDBC datasource to use this driver. For WebLogic, you will need to manually copy the appropriate JDBC driver jar file (included in the Cisco Prime Service Catalog

product image) to your WebLogic directory, and manually configure the JDBC datasource to use that driver. The instructions for configuring JDBC datasource for WebLogic are described later in this document.

Your database must be configured to enable TCP/IP for client connectivity.

The [Configuring the Service Catalog Database](#) contains instructions on how to create a database or schema for use with Prime Service Catalog.

## LDAP

Prime Service Catalog can be integrated with your corporate LDAP server to access your company's employee directory. This integration feature is optional, so an LDAP server is not a prerequisite software for installing Prime Service Catalog.

If you plan to use the LDAP integration feature, see the *Cisco Prime Service Catalog Integration Guide*. Ensure that you use only one of the supported LDAP software listed in [Table 2-1](#).

## IBM Cognos

OEM IBM Cognos software is available as an additional purchase, which is used for the (optional) Reporting module. To enable all Reporting and Advanced Reporting features in the Prime Service Catalog application, the Cognos software must be installed in your deployment topology. This software can be installed after the Prime Service Catalog software is installed. The instructions for installing and configuring Cognos software can be found in [Chapter 7, "Installing and Upgrading Reporting Module"](#)

## Other Miscellaneous Settings

### X-Window or Xvfb

The Service Catalog installer is a GUI program. Therefore if you are on a Linux Operating System, you must have either an X-Window Server or an X11 emulator to display the installation wizard. The Service Catalog installer does not support console mode or CLI mode.

You must also have either X-Window Server or Xvfb (virtual framebuffer X server) installed and running on your application server machine, in order for the KPI Charts in the Reporting module to be displayed properly on the browser. If you are not using the KPI Charts feature in the Reporting module, then X-Window Server is not required for the application server machine.

### Unzip Utility

You need to have an Unzip program (on Windows) or a GNU-compatible tar utility (on Linux) available on your machine to extract the Cisco Prime Service Catalog software installer package.

### Network – TCP/IP

TCP/IP must be configured on all host computers.

## SMTP

You should have access to an SMTP server that listens to port 25, and a valid email address, for email notifications from the Service Catalog to send out alerts to the system administrator. You must provide the SMTP address and a valid email address during the installation of the Prime Service Catalog software. The SMTP Server must not require user authentication.

# Hardware Requirements

## Sizing

We recommend a minimum of three computers for a typical (nonclustered) deployment topology:

- Web Server + Application Server together
- Database Server
- Reporting Server

**Note**


---

If you have a clustered application server environment, the hardware requirements specified above are applicable for each node (that is, each machine) in your clustered environment.

---

Your hardware configuration depends on site-specific factors. Contact the Cisco Technical Assistance Center (TAC) if you need more sizing recommendations.

The variables that can affect your hardware configuration include the following:

- the number of people who will use the system
- the number and frequency of service requests that the installed product will handle
- the nature of the service requests (complexity, type, and so on)
- reporting frequency
- systems integration and system availability requirements

## Minimum Hardware Requirements for Application Server Host

Your application server machine must meet the following minimum hardware requirements:

- 6 Core, 2 GHz (or faster) processor
- 10 GB RAM
- 100 GB *free* hard disk space
- There must be at least 2 GB of free disk space on the drive that contains the %TEMP% directory, if this is different from the drive when you plan to install the Cognos software.

## Minimum Hardware Requirements for Web Server Host

If your web server resides on a different machine from your application server, then your web server machine must meet the following minimum hardware requirements:

- 4 Core, 2 GHz (or faster) processor
- 4 GB RAM
- 2 GB *free* hard disk space

## Minimum Hardware Requirements for Database Host

Your database server machine must meet the following minimum hardware requirements:

- 8 Core, 2 GHz (or faster) processor
- 30 GB RAM
- Two hard disks with 500 GB *free* space. (Disk space requirement is dependent on the *projected* size of your Prime Service Catalog databases over time, to account for the growth in user data, service definitional data, transactional data, and reporting data.)

## Minimum Hardware Requirements for Reporting Server Host

Your Cognos machine must meet the following minimum hardware requirements:

- 4 Core, 2 GHz (or faster) processor
- 8 GB RAM
- 50 GB *free* hard disk space



---

**Note**

The IBM Cognos 10.2.1 software bundled with Prime Service Catalog can be installed only on a Microsoft Windows Server 2012 R2 (64-bit) Operating System.

---





## Configuring the Service Catalog Database

The Cisco Prime Service Catalog product requires an OLTP database, which is referred to as the ServiceCatalog database. The ServiceCatalog database can be manually created by the DBA prior to executing the Cisco Prime Service Catalog installer, or automatically created by the installer if the user selects the "Create Database" option on the installation wizard. The following sub-sections contain the manual instructions for creating the ServiceCatalog database on either Oracle or SQL Server.



### Note

The installer does not automatically create the Oracle tablespaces for you. It only creates a ServiceCatalog schema with a fixed size of 500 MB in the tablespaces specified by you on the installation wizard. Thus, even if you decide to let the installer create the ServiceCatalog schema automatically, you may still want to follow the instructions in the subsequent sections to prepare your Oracle server with the appropriate tablespaces, prior to running the Cisco Prime Service Catalog installer.

## Configuring Oracle

If you choose to use Oracle for your database, follow the instructions in this section to prepare the Oracle server and to create an Oracle user to be the owner of the ServiceCatalog schema.

### Oracle Parameters

Configure the following Oracle parameters:

**Step 1** Execute the following commands to find out the current values for the following Oracle parameters:

```
SHOW PARAMETER CURSOR_SHARING;
```

```
SHOW PARAMETERS PROCESSES;
```

```
SHOW PARAMETERS OPEN_CURSORS;
```

**Step 2** If CURSOR\_SHARING is not set to EXACT, use the following command to change it:

```
ALTER SYSTEM SET CURSOR_SHARING=EXACT SCOPE=BOTH SID='*';
```

**Step 3** If OPEN\_CURSORS is less than 1000, use the following command to change it:

```
ALTER SYSTEM SET OPEN_CURSORS = 1000 SID='*' SCOPE=BOTH;
```

- Step 4** If PROCESSES parameter is smaller than 500, then work with your DBA to bump up the PROCESSES parameter for your Oracle database to 500 (or higher).
- Step 5** Restart the Oracle instance to make sure that the new parameters take effect.
- 

## catcio.sql Package

- Step 1** Execute the following sql command as the Oracle “sys” user to find out if the catcio.sql package has been installed on the Oracle database:
- ```
select count(*) from all_tables where owner='SYS' and table_name like
'IND_ONLINE$';
```
- Step 2** If the returned value is ZERO, then log in to Oracle database as “sys” user (connect as “sysdba”), and install the catcio.sql package. This needs to be done before you proceed with the Prime Service Catalog installation. The catcio.sql script is usually located in the \$ORACLE\_HOME/rdbms/admin directory.
- 

## Redo Logs

Allocate at least three groups of Redo logs with two files each of 200 MB for Oracle.

## Unicode Character Set

For a new installation, you must configure the Oracle database to use one of the following Unicode characters sets: “AL32UTF8” or “AL16UTF16”.

To determine if the database character set is Unicode, execute the following sql command:

```
SELECT VALUE FROM NLS_DATABASE_PARAMETERS WHERE PARAMETER='NLS_CHARACTERSET';
```

If the value returned for the NLS\_CHARACTERSET parameter is neither “AL32UTF8” nor “AL16UTF16”, then you need to create a new Oracle database, and specify the character set to be either “AL32UTF8” or “AL16UTF16” at creation time.



**Note**

For an upgrade installation from release 9.x, the database character set does not have to be Unicode.

---

## Creating Tablespaces and Database Schema for Hosting Service Catalog Data

For a new installation, you can prepare the tablespaces and database schema as described in this section before executing the Service Catalog installer, or you can let the Service Catalog installer create the database schema on the default tablespaces for you by selecting the “Create Database” option presented by the installation wizard. The “Create Database” option of the Service Catalog installer is described in more detail in the [Installing Prime Service Catalog on WildFly Application Server](#) or [Installing Prime Service Catalog on WebLogic Application Server](#).

To create tablespaces and database schema:



- Step 1** Create a new tablespace named **SERVICECATALOG**, with initial size of 500 MB and AUTOEXTEND ON.
- Step 2** Create a new temporary tablespace named **SERVICECATALOG\_TEMP**, with initial size of 30 MB and AUTOEXTEND ON.
- Step 3** Create a database user named **CPSCUser**, with default tablespace set to **SERVICECATALOG** and temporary tablespace set to **SERVICECATALOG\_TEMP**. **CPSCUser** should be granted **QUOTA UNLIMITED** on the **SERVICECATALOG** tablespace.
- Step 4** Log in to the Oracle server as the "sys" user, and execute the following commands to grant the permissions to "CPSCUser":

```
GRANT
CREATE SESSION,
CREATE TABLE,
CREATE PROCEDURE,
CREATE SEQUENCE,
CREATE TRIGGER,
CREATE VIEW,
CREATE MATERIALIZED VIEW,
CREATE SYNONYM,
ALTER SESSION
TO CPSCUser;

GRANT EXECUTE ON DBMS_LOB TO CPSCUser;

COMMIT;
```

- Step 5** The permissions listed above are required for the normal operation of the Service Catalog application. There are some special permissions needed for the application to monitor and automatically recover from long-running queries that may affect the performance of the product. If these additional permissions are not granted to "CPSCUser", the product will not fail; but the user may see an error message in the application server's log file that is similar to the following.

```
ERROR [com.newscale.bfw.udkernel.udsql.UdSqlBean] (ajp--0.0.0.0-8009-1)
COR-ID=-7123843321231324051::SQL Exception while getting open session:
java.sql.SQLException: [newscale][Oracle JDBC Driver][Oracle]ORA-00942: table
or view does not exist
```

(Optional) To grant these special permissions, log in to the Oracle server as the "sys" user, and execute the following commands:

```
GRANT ALTER SYSTEM TO CPSCUser;
GRANT SELECT ON v_$session TO CPSCUser;
GRANT SELECT ON v_$mystat to CPSCUser;
COMMIT;
```



**Note** As an additional validation, the installer verifies if the database user is granted the optional privileges and if not, a warning message shows up indicating the missing privileges. Click OK to continue without the optional privileges or click Cancel to exit the installation. Not having the optional privileges does not cause the application to fail but limits its functionality.

## Configuring Oracle RAC 12C

If you want to perform database connection failover, you can use Oracle RAC 12C for your databases. For instructions to install Oracle RAC 12c, see Oracle documentation.

After you set up Oracle RAC , note down the cluster SCAN name and the service name. These parameters are required while configuring database during the Prime Service Catalog installation.

If you cannot use a DNS server or the DNS server is inaccessible on the Prime Service Catalog server, you must manually map the SCAN IP addresses to the SCAN name in the /etc/hosts file in that server. The following is an example of this mapping in the /etc/hosts file:

```
# SCAN Name to SCAN IP Mapping
<scan_ip-1> <scan_name>
<scan_ip-2> <scan_name>
<scan_ip-3> <scan_name>
```

Where:

*scan\_ip-x* is the SCAN IP address and *scan\_name* is the SCAN name.

## Configuring Microsoft SQL Server

If you choose to use Microsoft SQL Server for your databases, follow the instructions in this section to prepare the SQL Server, and to create the ServiceCatalog database.

### Default Instance or Named Instance

The SQL Server can be set up as a Default Instance or a Named Instance. The port number for each instance must be unique per database host.

### Mixed-Mode Authentication

The SQL Server must be configured to use mixed-mode authentication. This is because the Prime Service Catalog Installer needs to connect to the SQL Server as the "sa" user in order to create the Service Catalog schema.

## Creating ServiceCatalog Database and Login User

For a new installation, you can prepare the ServiceCatalog database and login user as described in this section before executing the Service Catalog installer, or you can let the Service Catalog installer create the database and login user for you by selecting the "Create Database" option presented by the installation wizard. The "Create Database" option of the Service Catalog installer is described in more detail in the [Installing Prime Service Catalog on WildFly Application Server](#) or [Installing Prime Service Catalog on WebLogic Application Server](#).

To create the ServiceCatalog database and login user:

---

**Step 1** Create a database named **ServiceCatalog** in the SQL Server, with the following settings for the data file

- Initial size = 1 GB.
- Autogrowth = 500 MB, unlimited

- Step 2** Set the collating sequence for the ServiceCatalog database to case-insensitive.
- Step 3** Put the ServiceCatalog database in SINGLE-USER mode, and execute the following command:  
ALTER DATABASE ServiceCatalog SET READ\_COMMITTED\_SNAPSHOT ON.
- Step 4** Put the ServiceCatalog database back in MULTI-USER mode.
- Step 5** Create a SQL Server Login named **CPSCUser**, with the Default Database property set to “ServiceCatalog”.



**Note** CPSCUser must be a SQL Server login account that authenticates to the SQL Server using SQL Server authentication method, and not Windows authentication method.

- Step 6** Ensure that the “Enforce Password Policy” option is unchecked in the Security setting properties for CPSCUser. Furthermore, the password for CPSCUser must contain only alphanumeric characters. For example, enter only letters and numbers for password. Do not enter any special characters like underlines, asterisks, brackets, and so on. Some combinations of these special characters may cause the installer to fail at product installation time with a “Database Connection Test failed” error message.
- Step 7** Assign this CPSCUser to be the **db\_owner** of the “ServiceCatalog” database. Verify your setting to ensure that:
- The user name “CPSCUser” in the ServiceCatalog database is mapped to the login name “CPSCUser” in the SQL Server
  - The default schema is “dbo”
  - The user name “CPSCUser” has the “db\_owner” database role membership.
- Step 8** There are some special permissions needed for the application to monitor and automatically recover from long-running queries that may affect the performance of the product. If these additional permissions are not granted to “CPSCUser”, the product will not fail; but the user may see some error messages in the application server's log file that are similar to the following:

```
ERROR [com.newscale.bfw.udkernel.udsql.UdSqlBean]
(org.springframework.scheduling.quartz.SchedulerFactoryBean#0_Worker-3) SQL Exception
while getting open session: java.sql.SQLException: [newscale][SQLServer JDBC
Driver][SQLServer]The user does not have permission to perform this action.
Error: Error while validation policiesjava.lang.Exception: Connection SessionId could
not be obtained exiting policy check for service item subscription
```

(Optional) To grant these special permissions, log in to the SQL Server as the “sa” user, and execute the following commands:

```
EXEC sp_addsrvrolemember 'CPSCUser', 'sysadmin'
GRANT ALTER ANY CONNECTION TO CPSCUser
GO
```

## Adding -T272 Property to SQL Server Database

When SQL Server is restarted, the requisition identity value jumps by 1000 after each restart of SQL Server. To resolve this issue, add the -T272 as the database property for the SQL Server database. This will force the identity column value to increment by 1 instead of 1000 each time the SQL Server is restarted.

- 
- Step 1** Open SQL Server Configuration Manager.
- Step 2** Click on the **SQL Server Services** in the left pane.
- Step 3** Right click on the SQL Server (MSSQLSERVER) to open the properties window.
- Step 4** In the **Startup Parameters** tab, enter -T272 in the **Specify a startup parameter** field and click **Add**.
- Step 5** Click **OK** to close the properties window.
- Step 6** For the changes to take effect, you must restart the SQL Server.
- 

## Setting Compatibility Mode

Since Prime Service Catalog 12.1 release supports both MS SQL Server 2012 and MS SQL Server 2016, ensure that database is set to the corresponding compatibility mode as below:

- MS SQL Server 2012 must be set to 110
- MS SQL Server 2016 must be set to 130

- 
- Step 1** Right click on the database and select **Options**.
- Step 2** Set the appropriate mode for the Compatibility Level field.
- Step 3** Click **OK** to save the settings.
-



## Setting Up WildFly Application Server

Cisco Prime Service Catalog is bundled with the WildFly-10.1.0.Final software distribution. If you select WildFly as the application server on the installation wizard, the installer will automatically install and deploy the WildFly software on the same machine where you are running the installer. You do not need to install the WildFly Application Server software as a prerequisite. We recommend that you let the Service Catalog installer install the WildFly software for you. The Cisco Prime Service Catalog installer will automatically install the WildFly Application Server and deploy the Service Catalog applications.

The WildFly application server can be configured in both standalone and cluster setup. The subsequent sections in this chapter describes various deployment topologies for WildFly Application Servers.

You can choose to install the Service Catalog and Service Link in two separate virtual machines using the **Standalone Custom** option. Always install the Service Catalog node first, followed by Service link on the second virtual machine. The Service Catalog node will have the WildFly application server instance with Service Catalog installation folder. To install Service Catalog and Service Link on the same virtual machine, either choose the **Standalone Typical** option or **Standalone > Custom > Both** options. In this case, the installer will create single WildFly instance with Service Catalog and Service Link folder under the WildFly application server. For setting up Prime Service Catalog in standalone mode for both Typical and Custom type, see [Setting Up WildFly Standalone Application Server](#).



### Note

Standalone Typical is recommended only for a demo or test system.

For setting up Wildfly application server in cluster for the failover scenarios, see [Setting Up WildFly Clustered Application Servers](#).

The JMS service is configured in the WildFly server where the Service Link component application resides.

Follow the instructions in the Preinstallation Configuration for WildFly section of this chapter to prepare your machine. Then after you execute the Cisco Prime Service Catalog installer, follow the Postinstallation Configuration for WildFly section of this chapter to verify your installation.

- [Preinstallation Tasks for WildFly, page 4-1](#)
- [Installing Prime Service Catalog on WildFly Application Server, page 4-6](#)
- [Postinstallation Tasks for WildFly, page 4-28](#)

## Preinstallation Tasks for WildFly

This section contains instructions for preparing your computer, prior to installing Prime Service Catalog with WildFly application server.

This release of Prime Service Catalog supports WildFly Application Server on the following Operating Systems, web servers, and Java Development Kit:

**Table 4-1 WildFly Supported Operating System, Web Server, and Java**

| WildFly Application Server | Operating System                             | Web Server                                        | Java                                                    |
|----------------------------|----------------------------------------------|---------------------------------------------------|---------------------------------------------------------|
| WildFly-10.1.0.Final       | Red Hat Enterprise Linux Server 7.3 (64-bit) | Red Hat Http Server 2.4.6                         | Red Hat OpenJDK 8 (version 1.8.0_131 or higher 1.8.0_x) |
| WildFly-10.1.0.Final       | Windows Server 2012 R2 (64-bit)              | Microsoft Internet Information Services (IIS) 8.5 | Oracle JDK 8 Update 131 (or higher update)              |

## Preinstallation Checklist

- Review the [Installation Requirements](#) to ensure that you have adequately addressed the minimum hardware and software requirements for running the system.
- Ensure that you have performed the database tasks described in the [Configuring the Service Catalog Database](#), and completed the [Database Information Worksheet](#).
- Ensure that you have performed the preinstallation tasks for your type of application server and completed the Application Server Information Worksheet in [Appendix A, “Worksheets”](#).
- The Cisco Prime Service Catalog installer requires Java 1.8. For the prerequisite details, see [“Installing Java” section on page 4-4](#).
- If you are on a Windows Operating System, stop the IIS web server.
- Extract the electronic software distribution file that you downloaded from the Cisco web site to your computer, if you have not already done so. For more information, see [Downloading Prime Service Catalog Software Image, page 4-5](#).
- Add the %JAVA\_HOME%\bin (or \$JAVA\_HOME/bin if you are on Linux) to the beginning of the PATH environment variable on your machine, where %JAVA\_HOME% points to the correct JDK directory.
- The Cisco Prime Service Catalog installer is a GUI program. On Linux Operating System, you will need a graphical display, such as X-window. The installer does not support console mode or CLI mode.
- During the installation, you will be asked to specify the destination directory for the software.
  - On Windows, the default destination directory is "C:\CiscoPrimeServiceCatalog".
  - On Linux, the default destination directory is "/opt/CiscoPrimeServiceCatalog". Ensure that there is at least 2 GB free disk space in the destination directory; otherwise, the installer will display the following error message:
 

```
Not enough disk space.
The installation requires 2048 MB of free disk space, but there are only 182 MB
available at C:\CiscoPrimeServiceCatalog.
Please free the required space to proceed with the installation.
```
- During installation, the installer requires an additional 2 GB of free disk space in the TMP directory, where it extracts some temporary files. The TMP directory is different for different Operating Systems and/or user profiles.
  - On Windows, the TMP directory is the %TMP% or %TEMP% environment variable for the user profile.

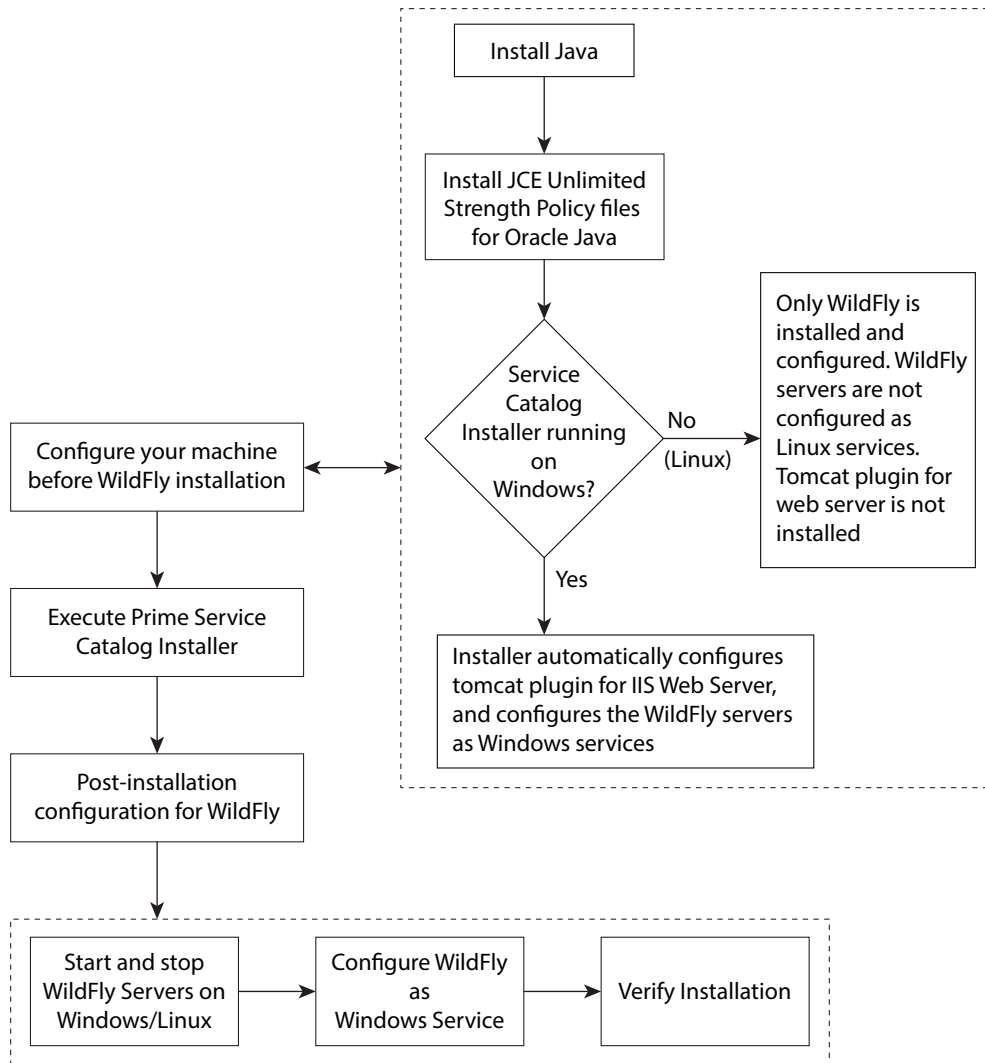
On Linux, the TMP directory is usually either /tmp or /var/tmp directory.

- Ensure that JBOSS\_HOME is not set as an environment variable in the system.
- Ensure that you size your application server machine based on defined parameters listed in section [Minimum Hardware Requirements for Application Server Host, page 2-6](#).

## WildFly Installation Flow

The following figure illustrates steps to install Prime Service Catalog on WildFly Application Server.

**Figure 4-1** Installation Flow for WildFly Application Server



364204

## Installing Java

In this section, you will install JDK as a prerequisite, and prepare the environment variables on your computer.


**Note**

If you are on Windows Server, you must install Oracle JDK as a prerequisite, plus the JCE Unlimited Strength Policy jar files. If you are on Red Hat Enterprise Linux Server, you must install Red Hat OpenJDK as a prerequisite. You don't need JCE Unlimited Strength Policy jars for Red Hat OpenJDK.

## Oracle JDK

- Step 1** Download Oracle JDK 8 Update 77 (or higher Update) from the Oracle website. Ensure that you download the correct version of JDK 8. Only Update 77 or later is supported.


**Note**

During the installation, the installer prompts for the Java path and this prompt appears only for WildFly, and not for WebLogic. However the installer does not use the JAVA\_HOME path that you enter in this screen to launch its own Java process, but uses the Java executable that it finds in the PATH environment variable of the Operating System.

- Step 2** Copy the unlimited strength JCE policy files to the %JAVA\_HOME%\jre\lib\security directory, overwriting the existing files. The unlimited strength policy files are "local\_policy.jar" and "US\_export\_policy.jar", which can be downloaded from the following link:

<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>

- Step 3** Add the <path\_to\_oracle\_jdk\_1.8\_java\_executable> to the PATH environment variable. You may have multiple Java installation on your machine. Make sure that the path to the Java executable for Oracle JDK 1.8.0\_x is first in the PATH environment variable. This is what the Prime Service Catalog installer will use when it is first launched.


**Note**

By default, after successful installation of JDK 1.8, the value *C:\ProgramData\Oracle\Java\javapath* is updated in the path variable (environment variables). You must remove this manually and add the appropriate installed java folder.

For example:

```
set JAVA_HOME=C:\jdk1.8.0_77
set PATH=%JAVA_HOME%\bin;%PATH%
```

## Red Hat OpenJDK

- Step 1** Install OpenJDK on your Red Hat Enterprise Linux Server by executing the "yum install java-1.8.0-openjdk-devel" command.


**Note**

You must have Red Hat license and subscription in order to do "yum install".



- Step 2** Add the <path\_to\_openjdk\_1.8\_java\_executable> to the PATH environment variable. You may have multiple Java installation on your machine. Just make sure that the path to the Java executable for OpenJDK 1.8.0\_x is first in the PATH environment variable. This is what the Prime Service Catalog installer will use when it is first launched.

For example:

- export JAVA\_HOME=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.85-2.6.1.2.el7\_1.x86\_64
  - export PATH=\$JAVA\_HOME/bin:\$PATH
- 

## Preparing IIS Web Server

If you are running the Service Catalog installer on a Windows Operating System, the installer can automatically configure the tomcat plugin for the IIS web server, and configure the Wildfly servers as Windows services. The options for "Configure IIS" and "Configure windows services" are presented on the installation wizard, and you can select or deselect each option as you desire.

If you want the Service Catalog installer to configure the tomcat plugin for the IIS web server, then you need to perform the following prerequisite tasks:

- Install IIS on the same Windows Operating System where you plan to execute the installer.
- Add the following role services for IIS: ISAPI Extensions, ISAPI Filters.  
For more information on adding role services, see the IIS documentation on [www.iis.net](http://www.iis.net).
- Stop the World Wide Web Publishing Service prior to executing the Service Catalog installer.
- You will be prompted to enter the name of the IIS web site. You can enter either "Default Web Site" or the name of another web site. If you enter the name of another website, then you must create that website as a prerequisite.

If you are running the Service Catalog installer on a Linux Operating System, then the installer will install only the WildFly software. It will not configure the tomcat plugin for the Http web server, and will not configure the WildFly servers to run as Linux services.

## Downloading Prime Service Catalog Software Image

In this section, you will download the electronic software distribution for Prime Service Catalog.

- 
- Step 1** Access the Cisco product download web site and authenticate with the user name and password provided to you.
- Step 2** Search by product name, or navigate within the product selector to locate the product you want to download. (Navigation: **Downloads Home** > **Products** > **Cloud and Systems Management** > **Service Catalog** > **Prime Service Catalog**).
- Step 3** A list of different releases is displayed. Locate Prime Service Catalog 12.1 and click it.
- Step 4** Click the Prime Service Catalog Software link. Then click the link for the appropriate operating system.
- Step 5** Download file CPSC\_12.1\_win.zip for the Windows Operating System, or file CPSC\_12.1\_linux.tar.gz for the Linux Operating System.

**Note**

If you are installing the Prime Service Catalog 12.1 Virtual Appliance, you need to click the link called VMware for Operating System, then download the OVA file. Do not use this guide for installation instructions. Refer to the *Prime Service Catalog Quick Start Guide* for the installation instructions for the Virtual Appliance.

**Step 6**

Extract the software image to a directory on your application server machine.

**Note**

The CPSC\_12.1\_linux.tar.gz file must be untarred using a GNU-compatible tar utility. Older tar utilities may have problems unzipping tar files that contain filenames longer than 100 characters.

## Installing Prime Service Catalog on WildFly Application Server

After your WildFly environment is prepared, proceed to configure WildFly application server in one of the following modes:

- [Setting Up WildFly Standalone Application Server, page 4-6](#)
- [Setting Up WildFly Clustered Application Servers, page 4-10](#)

### Setting Up WildFly Standalone Application Server

Prime Service Catalog standalone installation provides two installation types —Typical and Custom. The Typical installation performs a streamlined installation using default settings. It requires a smaller footprint as the three foundational application components—Service Catalog application, Service Link application, and JMS service—are hosted on the same application server. Typical installation is commonly used when setting up a sandbox environment.

The Custom installation allows you to configure a different deployment topology and to apply custom changes to the application. Using the custom option, you can choose to install only the Service Catalog component application on your computer, only the Service Link component application on your computer, or both Service Catalog and Service Link component applications together on the same computer.

When you choose to install both component applications together on the same computer, the installer will always create only one WildFly server instances, for both Service Catalog and Service Link component.

The JMS service is configured in the WildFly server where the Service Link component application resides.

- Have separate tablespaces for definitional data, transactional data and indexes (for Oracle Only)
- Add custom content to the RequestCenter.war
- Recreate the RequestCenter.war or ISEE.war files without executing any database scripts
- For WildFly, the Custom mode allows the user to install "Service Catalog only", "Service Link only" or "both"

For information about performing an upgrade installation, see [Chapter 6, “Upgrading Prime Service Catalog”](#).

## Performing a Standalone Installation For WildFly Application Server

### Before You Begin

Verify all the other preinstallation tasks are completed before proceeding with the installation. The preinstallation tasks are summarized in [Preinstallation Checklist, page 4-2](#).

### Procedure

- 
- Step 1** Launch the web interface installation wizard.
- On Windows Operating System, log in as a user with administrator rights and double-click `setup.cmd`.
  - On Linux Operating System, log in as the root user and execute `./setup.sh` from a graphical interface, such as X-window.
- Step 2** When the Introduction panel appears, click **Next**.
- Step 3** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.
- On Windows, the default value for destination folder is `C:\CiscoPrimeServiceCatalog`.
  - On Linux, the default value is `/opt/CiscoPrimeServiceCatalog`. The value for destination directory must not contain any space character.
- Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`. For WildFly, this directory is also where the Service Catalog installer installs and configures the WildFly Application Server software.
- Step 4** On the Application Server Selection panel, select the application server **WildFly** and click **Next**.
- Step 5** On the Setup Mode Selection panel, select **Standalone** radio button and click **Next**.
- Step 6** Depending on your requirements, select one of the following and click **Next**.
- **Typical**. Use the typical installation if you want to perform a streamlined installation using default settings. Service Catalog application, Service Link application, and JMS service—are hosted on the same application server.
  - **Custom**. Use the custom installation if want to customize various aspects of the installation rather than accepting the defaults.
- Step 7** (For Custom Installation Type Only) Select a component in the Component Selection panel and click **Next**.
- The Custom installation mode for WildFly allows you to install
- only the Service Catalog server,
  - only the Service Link server, or
  - both Service Catalog and Service Link servers on the same computer.
- The custom installation type allows you to install Service Catalog and Service Link on different virtual machines or on the same virtual machine.
- Step 8** On the Database Selection panel, select a database platform (Microsoft SQL Server or Oracle) and click **Next**.

The subsequent panels may look different depending on which database platform you select at this point. Refer to the [Database Information Worksheet](#) that you filled out in Appendix A to determine your database platform.

**Step 9** On the Service Catalog Database Creation panel:

- If you have not created the database in advance, select **Yes**. By selecting **Yes**, you are telling the installer to create the database automatically for you. In the next panel, you will be prompted for the information that the installer will use to create the database user and database schema for Service Catalog. Refer to the [Database Information Worksheet](#) for the description of each field on this panel.
- If you have already created your database, then select **No**. In the next panel, you will be prompted for the information of the existing database user and database schema. Refer to the [Database Information Worksheet](#) for the description of each field on this panel. (If you are performing an upgrade installation, you must select No. Refer to Chapter 7: [Upgrading Prime Service Catalog](#) for more detailed information).

**Step 10** On the Service Catalog Database panel, enter the information for the Service Catalog database.

- If you selected **Yes** in [Step 9](#), you will see a **Create Database** button on this panel, and the Next button is grayed out.

Notice that you need to enter the password for either the “sys” user (for Oracle) or the “sa” user (for SQL Server) which the installer will use to connect to your database server. Once you enter the information on this panel, click **Create Database**. If you get the message “*Service Catalog database created successfully*,” click **OK** to close the message. The **Next** button is now enabled.

- If you selected **No** in [Step 9](#), enter the details of the existing Service Catalog database, and select the **Execute database scripts** check box.




---

**Note** The “Create Database” feature creates a very basic Service Catalog database that meets the minimum requirements for the Service Catalog application to operate. This feature is recommended for a Demo or Test system. For a Production system, contact your DBA in advance, to create the Service Catalog database which meets all of the product requirements as described in the Configuring Databases section, as well as any performance, reliability, and security requirements that adhere to your corporate policy.

---

**Step 11** Click **Next** to continue.

The installer connects to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if any database setting is missing. See the [Software Requirements](#) for the database requirements. If a database validation error occurs, you can do the following:

- Close the error dialog and click **Cancel** to exit the installation wizard, or
- Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next panel.

**Step 12** On the Master Key Password panel, enter the master key password.

As part of the security requirement, a master key password must be provided that would be used to encrypt all the passwords that are available in the application. The password provided must match the password rules, as described on the panel.

The master key password is saved in two files, `kek_new.txt` and `kek_old.txt`, under the `<ServiceCatalog_Install_Dir>/dist` directory. The `kek_new.txt` and `kek_old.txt` files must be backed up and stored in a safe location. The application server cannot login to the ServiceCatalog database without the master key password files. If you lose these master key password files, please contact Cisco TAC for help.

- Step 13** On the Choose Java Virtual Machine panel, select the correct Java JDK version 1.8.0\_x from the list or click the **Search Another Location** button to navigate to the correct location of Java JDK version 1.8.0\_x on your computer and click **Next**.



**Note** You must specify the location of Java for WildFly because the installer will install the WildFly Application Server software on your computer, and it will set the `JAVA_HOME` variable in the WildFly configuration to use this particular Java.

- Step 14** On the Service Catalog Configuration panel, do the following and click **Next**.
- Enter the information for the WildFly server where the Service Catalog application (i.e. `RequestCenter.war`) will be deployed. Refer to the [Service Catalog Configuration Table for WildFly](#) for the description of each field on this panel.
  - (For Custom Installation Type Only) Click the **Advanced Options** button. Enter the information on the Advanced Options window, see [Advanced Options Table for Service Catalog Configuration panel](#) for reference and click **Close**.
  - Click the **Change Ports** button if you want to change any of the default port numbers assigned to the WildFly server for Service Catalog Configuration panel for reference and click **Close**.

- Step 15** On the Service Link Configuration panel, do the following and click **Next**.
- Enter the information for the WildFly server where Service Link application (i.e. `ISEE.war`) will be deployed. Refer to the [Service Link Configuration Table for WildFly](#) for the description of each field on this panel
  - Click the **Change Ports** button if you want to change any of the default port numbers assigned to the WildFly server for Service Link and click **Close**.

- Step 16** On the Messaging Configuration panel, enter the information for the JMS Queue server and click **Next**. Refer to the [Messaging Configuration Table](#) for the description of each field on this panel.



**Note** The JMS Queue server will always be installed on Service Link server.

- Step 17** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.

- Step 18** Click **Install** in the Pre-Installation Summary panel to begin installation.

The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.

- Step 19** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.

- Step 20** Configure the web server.

If you selected the **Configure IIS** option on both the Service Catalog Configuration panel and the Service Link Configuration panel during the installation, then the IIS web server on your VM was automatically configured by the Prime Service Catalog Installer to point to the WildFly servers. You can connect to the Service Catalog UI with the following URL:

`http://<web_server_host>: port/RequestCenter,`

where:

`<web_server_host>` is the IP address of your VM.

If you are on Linux operating system, then the Prime Service Catalog Installer does not automatically configure the web server for you. You have to install either the Apache web server or the IIS web server (on a Windows machine) and configure it to point to the WildFly server for Service Catalog.

Refer to the **Configure Web Server for WildFly** document for instructions on how to configure web server.

## Next Steps

Perform [Postinstallation Tasks for WildFly, page 4-28](#).

## Setting Up WildFly Clustered Application Servers

The Prime Service Catalog WildFly cluster configuration comprises of a Domain Controller, Service Link with JMS service, and two Host Controllers for cluster nodes - Host 1 and Host 2 that host the RequestCenter.war file.

A two node cluster means that there are two horizontal nodes (i.e. two separate hosts) that belong to a WildFly cluster configuration. The user can start with two nodes, and add more nodes (i.e. more hosts) to the cluster, if desired. The Prime Service Catalog Installer will support only up to 6th node for the cluster. To add a 7th node or more, please contact Cisco TAC for manual instructions.



### Note

Only the Host Controllers that host the RequestCenter.war can be configured as clusters. Service Link application with JMS service cannot be deployed in a cluster. JMS service resides with the Service Link server.

Prime Service Catalog installer supports two types of cluster topologies for WildFly application server.

- **Two VM Topology.** Requires minimum of two virtual machines: In this configuration, first virtual machine includes a Domain Controller, Service Link Component, and host controllers for the Host 1. Second virtual machine includes only an host controller for the Host 2. For more information on setting this type of cluster, see [Performing WildFly Cluster Installation for Two VM Topology](#).
- **Four VM Topology.** Requires a minimum of four virtual machines: In this configuration, first virtual machine is for the Domain Controller, second virtual machines for the Service Link Component with JMS service, third virtual machine is for the host controller for the Host 1, and fourth virtual machine is for the host controller for the Host 2. For more information on setting this type of cluster, see [Performing WildFly Cluster Installation for Four VM Topology](#).



### Note

After you initiate the installation of a particular topology type, you cannot modify the configurations at a later stage. You can only add new nodes for the host controllers.

## Performing WildFly Cluster Installation for Two VM Topology

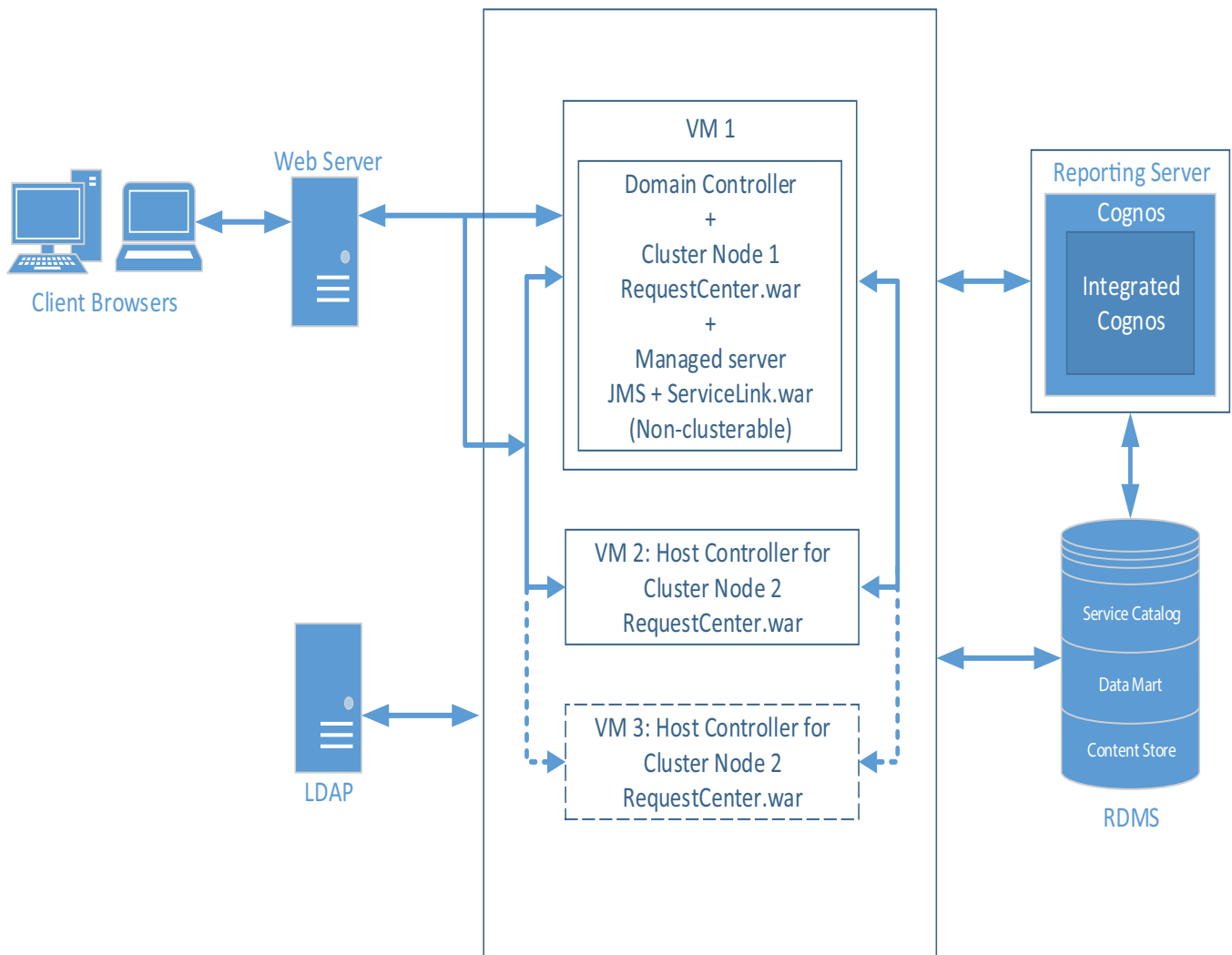


**Note**

This is an overview procedure for setting up two VM topology and the detailed setup instructions are described in the subsequent sections. To complete the setup, you must perform all the steps described in this overview procedure.

In the two VM topology, Domain Controller, Host Controller for Host 1, Service Link application with JMS service are installed on the first virtual machine and Host Controller for Host 2 is installed on the second virtual machine. The two VM topology diagram is shown below.

**Figure 4-2 Two VM Topology**



406036

## Before You Begin

Verify all the other preinstallation tasks are completed before proceeding with the installation. The preinstallation tasks are summarized in [Preinstallation Checklist, page 4-2](#).

## Procedure

- 
- Step 1** Prepare the database server.
- Make sure database server meets all the requirements. For more information, see [Configuring the Service Catalog Database](#), and completed the [Database Information Worksheet](#).
- Step 2** Prepare the virtual machines.
- Make sure both the virtual machines meet all the hardware and software requirements. For more information, see the [Installation Requirements](#). Plan the requirements such that Host 1 and Host 2 can include the following components:
- Host 1: Domain Controller, Host Controller 1 for Service Catalog, Service Link and JMS
  - Host 2: Host Controller 2 for Service Catalog
- Step 3** Set up Host 1. For more information on how to set up the Host 1, see the instructions in [Setting Up the Host 1 in Two VM Topology](#) procedure.
- Step 4** Set up Host 2. For more information on how to set up the Host 2, see the instructions in [Setting Up the Host 2 in Two VM Topology](#) procedure.
- Step 5** Install the Web Server.

Install the Apache web server, and configure it to point to the Cluster WildFly server group where RequestCenter.war was deployed. You must have a web server that acts as a load balancer on top of the cluster. All client connection to Service Catalog must go through the web server. Thus, the URL for Service Catalog will be

*[http://<web\\_server\\_host>:<web\\_server\\_port>/RequestCenter](http://<web_server_host>:<web_server_port>/RequestCenter)*

You can install the web server on its own VM, or if you'd like, you can install it on any of the existing VM because it won't interfere with the configuration of the other components that you have already installed in the previous steps.




---

**Note** Prime Service Catalog Installer does not install or configure the web server. You have to install the web server on your own. For configuring the Apache web server as a common web server for Service Catalog and Service Link, see [Setting Up Apache Web Server on WildFly](#).

---

If you selected the "Configure Windows Service" option during the installation, stop all the WildFly servers on VM1, VM2 and start them up again as windows services.

To stop the WildFly servers on VM1 or VM2, open the Command Prompt window, where startServiceCatalogCluster.cmd is running, and press **Control-C** to stop the process and start the windows service called - **Cisco Prime Service Catalog**.

- Step 6** (Optional) Add another node to the cluster.
- If you want to add a third node to the cluster, repeat [Step 4](#) for setting up Host 3. After setting up Host 3, modify the Plugin settings for the web server that you set up in [Step 5](#), so that it is aware of the third cluster node.



**Note**

You can execute the Prime Service Catalog Installer to add up to a 4th node to the cluster. If you want to add a 7th node or more, you need to contact Cisco TAC for manual instructions.

## Setting Up the Host 1 in Two VM Topology

- Step 1** On the machine designated for Host 1, launch the web interface installation wizard:
- On Windows Operating System, log in as a user with administrator rights and double-click `setup.cmd`.
  - On Linux Operating System, log in as the root user and execute `./setup.sh` from a graphical interface, such as X-window.
- Step 2** When the Introduction panel appears, click **Next** to begin.
- Step 3** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.
- On Windows, the default value for destination folder is `C:\CiscoPrimeServiceCatalog`.
  - On Linux, the default value is `/opt/CiscoPrimeServiceCatalog`. The value for destination directory must not contain any space character.
- Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`. For WildFly, this directory is also where the Service Catalog installer installs and configures the WildFly Application Server software.
- Step 4** On the Application Server Selection panel, select the application server as **WildFly** and click **Next**. The subsequent panels may look different depending on which application server you select at this point. Refer to the Application Server Information Worksheet that you filled out in Appendix A.
- Step 5** On the Setup Mode Selection panel, select **Cluster setup** radio button and click **Next**.
- Step 6** On the Node Type Selection panel, select **Cluster-ready complete installation** radio button and click **Next**.
- This option will install the Domain Controller, Host Controller for Host 1, Service Link and JMS on the Host 1.
- Step 7** On the Database Selection panel, select a database platform (Microsoft SQL Server or Oracle) and click **Next**. The subsequent panels may look different depending on which database platform you select at this point. Refer to the [Database Information Worksheet](#) that you filled out in Appendix A to determine your database platform.
- Step 8** On the Service Catalog Database Creation panel:
- If you have not created the database in advance, select **Yes**.  
By selecting **Yes**, you are telling the installer to create the database automatically for you. In the next panel, you will be prompted for the information that the installer will use to create the database user and database schema for Service Catalog. Refer to the [Database Information Worksheet](#) for the description of each field on this panel.
  - If you have already created your database or if you want to upgrade to an existing database, then select **No**.

In the next panel, you will be prompted for the information of the existing database user and database schema. Refer to the [Database Information Worksheet](#) for the description of each field on this panel. (If you are performing an upgrade installation, you must select No. Refer to Chapter 7: [Upgrading Prime Service Catalog](#) for more detailed information).

**Step 9** On the Service Catalog Database panel, enter the information for the Service Catalog database.

- If you selected **Yes** in [Step 8](#), you will see a **Create Database** button on this panel, and the **Next** button is grayed out.

Notice that you need to enter the password for either the “sys” user (for Oracle) or the “sa” user (for SQL Server) which the installer will use to connect to your database server. Once you enter the information on this panel, click the **Create Database**. If you get the message “*Service Catalog database created successfully*,” click **OK** to close the message. The **Next** button is now enabled.

- If you selected **No** in [Step 8](#), you just need to fill out the information for the existing Service Catalog database, and select the **Execute database scripts** check box.



**Note**

---

The “Create Database” feature creates a very basic Service Catalog database that meets the minimum requirements for the Service Catalog application to operate. This feature is recommended for a Demo or Test system. For a Production system, contact your DBA in advance, to create the Service Catalog database which meets all of the product requirements as described in the Configuring Databases section, as well as any performance, reliability, and security requirements that adhere to your corporate policy.

---

**Step 10** Click **Next** to continue. The installer connects to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if any database setting is missing. See the [Software Requirements](#) for the database requirements. If a database validation error occurs, you can do the following:

- Close the error dialog and click **Cancel** to exit the installation wizard.
- Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next panel.

**Step 11** In the Master Key Password panel, enter the master key password, if you selected **Yes** in step 8. Otherwise, enter the path to an existing KEK file that contains the Master Key Password for the existing database that you want to upgrade

As part of the security requirement, a master key password must be provided that would be used to encrypt all the passwords that are available in the application. The password provided must match the password rules, as described on the panel.

The master key password is saved in two files, `kek_new.txt` and `kek_old.txt`, under the `<ServiceCatalog_Install_Dir>/dist` directory. The `kek_new.txt` and `kek_old.txt` files must be backed up and stored in a safe location. The application server cannot login to the ServiceCatalog database without the master key password files. If you lose these master key password files, please contact Cisco TAC for help.

**Step 12** On Choose Java Virtual Machine panel, select the correct Java version for your platform. Click the **Search Another Location** button to navigate to the correct location of Java on your computer and click **Next**.



**Note** You must specify the location of Java for WildFly because the installer will install the WildFly Application Server software on your computer, and it will set the JAVA\_HOME variable in the WildFly configuration to use this particular Java.

- Step 13** On the Service Catalog Configuration panel, enter the information for the WildFly server (IP address of this machine, i.e, Host 1) where the Service Catalog application (i.e. RequestCenter.war) will be deployed. Refer to the [Service Catalog Configuration Table for WildFly](#) for the description of each field on this panel. Click **Next**.
- Step 14** On the Service Link Configuration panel, enter the information for the WildFly server (IP address of this machine, i.e, Host 1) where Service Link application (i.e. ISEE.war) will be deployed. Refer to the [Service Link Configuration Table for WildFly](#) for the description of each field on this panel. Click **Next**.
- Step 15** On the Messaging Configuration panel, enter the information for the JMS Queue server and click **Next**. Refer to the [Messaging Configuration Table](#) for the description of each field on this panel.
- Remember the Queue password value that you would fill in the Messaging Configuration panel, as you need to enter same password when you install the 2nd node on VM 2 later.
- Step 16** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.
- Step 17** Click **Install** in the Preinstallation Summary panel to begin installation.
- The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.
- Step 18** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.
- Step 19** Start the Domain Controller and all managed servers on the Host 1.



- Note**
- For the first time after the installation, each WildFly server must be started as an application by executing the start script provided by Cisco, as also described in this step. DO NOT use the windows service called Cisco Prime Service Catalog to start the server.
  - This start script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service.

To start the cluster services for the first time on any of the nodes, do the following:

- Access the `<ServiceCatalog_Install_Dir>\bin` directory.
 

```
cd <ServiceCatalog_Install_Dir>\bin
```
- Execute the following command to start the Domain Controller, Service Catalog, and Service Link:
 

[For Windows]:

```
startServiceCatalogCluster.cmd
```

[For Linux]

```
startServiceCatalogCluster.sh
```

This command will automatically start a total of 4 JVM processes on the Host 1:

- The Domain Controller
- The Process Controller
- A managed server for Service Catalog. This managed server belongs to a cluster server group called “main-server-group”. (Note that for this configuration, there is no need to have a separate Host Controller server since the Domain Controller will also act as a Host Controller for the managed server.)
- A managed server for Service Link. This managed server belongs to another server group called “other-server-group”. JMS is configured on this server.

**Step 20** Deploy RequestCenter.war and ISEE.war on Host 1. To start the cluster services for the first time on VM1, do the following:

- Access the `<ServiceCatalog_Install_Dir>\bin` directory.
- Execute the following command to the RequestCenter.war:

[For Windows]:

```
deployServiceCatalogCluster.cmd ALL
```

[For Linux]

```
deployServiceCatalogCluster.sh ALL
```

This command will push the RequestCenter.war to the cluster server group.

At this point, RequestCenter.war is deployed into a cluster server group called “main-server-group”. This cluster server group already contains one managed server. Thus, RequestCenter.war will be deployed immediately to the managed server for Service Catalog.

ISEE.war is deployed into a server group called “other-server-group”. This server group already contains one managed server. Thus, ISEE.war will be deployed immediately to the managed server for Service Link.

You can start and stop individual servers in a cluster. For information on the other start and stop scripts available with the installer for the WildFly cluster environment, see [WildFly Scripts](#). To stop the domain controller and all the managed servers on Host 1, execute the `shutdownAllOnHC1` script to stop both the domain controller, process controller, and the managed server for Service Catalog and Service Link.

### Next Step

Proceed to setting up the second node in the cluster. See [Setting Up the Host 2 in Two VM Topology](#).

## Setting Up the Host 2 in Two VM Topology

- Step 1** On the machine designated for Host 2, launch the web interface installation wizard:
  - On Windows Operating System, log in as a user with administrator rights and double-click `setup.cmd`.
  - On Linux Operating System, log in as the root user and execute `./setup.sh` from a graphical interface, such as X-window.
- Step 2** When the Introduction panel appears, click **Next** to begin.
- Step 3** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.

- On Windows, the default value for destination folder is **C:\CiscoPrimeServiceCatalog**.
- On Linux, the default value is **/opt/CiscoPrimeServiceCatalog**. The value for destination directory must not contain any space character.

Throughout this document, this destination folder is referred to as *<ServiceCatalog\_Install\_Dir>*.

For WildFly, this directory is also where the Service Catalog installer installs and configures the WildFly Application Server software.

- Step 4** On the Application Server Selection panel, select the application server as **WildFly** and click **Next**. The subsequent panels may look different depending on which application server you select at this point. Refer to the Application Server Information Worksheet that you filled out in Appendix A.
- Step 5** On the Setup Mode Selection panel, select **Cluster setup** radio button and click **Next**.
- Step 6** On the Node Type Selection panel, select **Host Controller Node** radio button and click **Next**.
- Step 7** On the Host Controller Selection panel, select **Host2** radio button and click **Next**.




---

**Note** Host 1 is the first node where Domain Controller, Service Link were installed. Second machine is the Host 2 in this cluster topology, so it is important that you select Host 2 here.

---

- Step 8** Enter the Domain Controller IP Address to establish connection to the first machine where domain controller is installed.
- Step 9** On Choose Java Virtual Machine panel, select the correct Java version for your platform. Click the **Search Another Location** button to navigate to the correct location of Java on your computer and click **Next**.




---

**Note** You must specify the location of Java for WildFly because the installer will install the WildFly Application Server software on your computer, and it will set the JAVA\_HOME variable in the WildFly configuration to use this particular Java.

---

- Step 10** On the Service Catalog Configuration panel, enter the information for the WildFly server (IP address of this machine, i.e, Host 2) where the Service Catalog application (i.e. RequestCenter.war) will be deployed. Refer to the [Service Catalog Configuration Table for WildFly](#) for the description of each field on this panel. Click **Next**.
- Step 11** On the Messaging Configuration panel, enter the information for the JMS Queue server and click **Next**. Refer to the [Messaging Configuration Table](#) for the description of each field on this panel.
- In the Queue password field, enter the same password that you entered for "Queue password" during the installation of the Domain Controller on Host 1.
- Step 12** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.
- Step 13** Click **Install** in the Preinstallation Summary panel to begin installation.
- The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.
- Step 14** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.
- Step 15** Start the Host Controller for Host 2.

**Note**

- For the first time after the installation, each WildFly server must be started as an application by executing the start script provided by Cisco, as also described in this step. DO NOT use the windows service called Cisco Prime Service Catalog to start the server.
- This start script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service.

To start the cluster services for the first time on any of the nodes, do the following:

- a. Access the `<ServiceCatalog_Install_Dir>\bin` directory.

```
cd <ServiceCatalog_Install_Dir>\bin
```

- b. Execute the following command to start the Domain Controller, Service Catalog, and Service Link:

[For Windows]:

```
startServiceCatalogCluster.cmd
```

[For Linux]

```
startServiceCatalogCluster.sh
```

The Host Controller will in turn, automatically start the managed server that belongs to the server group “main-server-group”. Since RequestCenter.war was already deployed in the “main-server-group” on the Domain Controller, it will also be automatically deployed onto this managed server.

You can start and stop individual servers in a cluster. For information on the other start and stop scripts available with the installer for the WildFly cluster environment, see [WildFly Scripts](#). To stop the host controller for VM2, execute the `forceStopAllOnHC` script to stop both the process controller and the managed server for Service Catalog.

**Next Step**

Set up web server. See [Step 5 of Performing WildFly Cluster Installation for Two VM Topology](#).

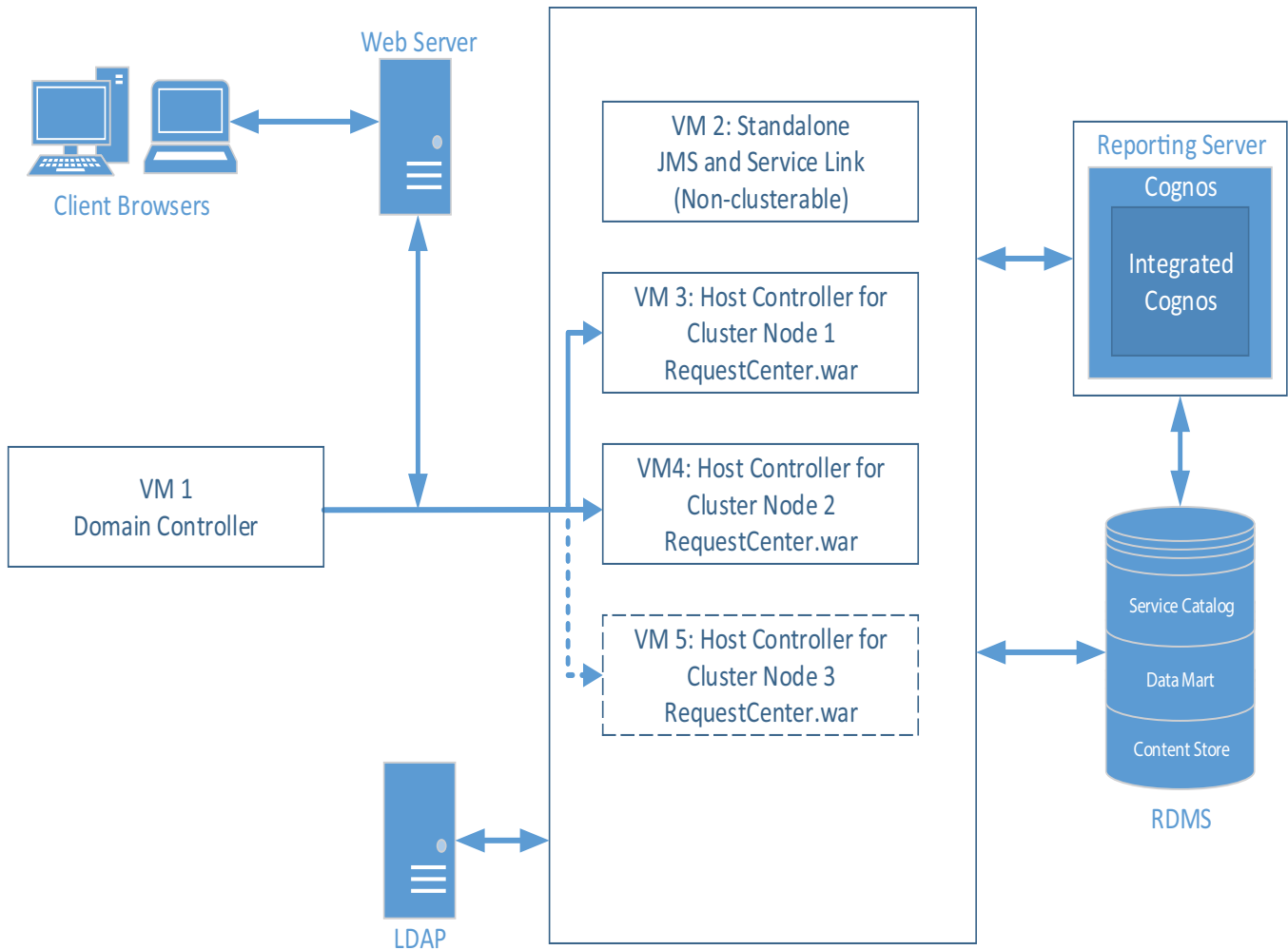
## Performing WildFly Cluster Installation for Four VM Topology

**Note**

This is an overview procedure for setting up four VM topology and the detailed setup instructions are described in the subsequent sections. To complete the setup, you must perform all the steps described in this overview procedure.

In the four VM topology, Domain Controller, Host Controller for Host 1 and Host 2, Service Link application with JMS service are installed on separate virtual machines. The four VM topology diagram is shown below.

Figure 4-3 Four VM Topology



406035

## Before You Begin

Verify all the other preinstallation tasks are completed before proceeding with the installation. The preinstallation tasks are summarized in [Preinstallation Checklist](#), page 4-2.

## Procedure

**Step 1** Prepare the database server.

Make sure database server meets all the requirements. For more information, see [Configuring the Service Catalog Database](#), and completed the [Database Information Worksheet](#).

**Step 2** Prepare the virtual machines.

Make sure all the virtual machines meet all the hardware and software requirements. For more information, see the [Installation Requirements](#). Plan the requirements such that following can be installed on each of the VMs:

- VM1:Domain Controller

- VM2: Service Link and JMS
- VM3: Host Controller 1 for Service Catalog
- VM4: Host Controller 2 for Service Catalog

- Step 3** Set up VM 1 as Domain Controller. For more information on how to set up domain controller, see the instructions in [Setting Up the Domain Controller Node \(VM 1\) in a Four VM Topology](#).
- Step 4** Set up VM 2 for Service link and JMS. For more information on how to set up Service Link and JMS node, see the instructions in [Setting Up the Service Link and JMS Node \(VM 2\) in a Four VM Topology](#).
- Step 5** Set up VM3 as Host Controller 1 for Service Catalog. For more information on how to set up Host Controller 1 for cluster nodes, see the instructions in [Setting Up Host Controller and Service Catalog For Cluster Nodes in a Four VM Topology](#).
- Step 6** Set up VM4 as Host Controller 2 for Service Catalog. For more information on how to set up Host Controller 2 for cluster nodes, see the instructions in [Setting Up Host Controller and Service Catalog For Cluster Nodes in a Four VM Topology](#).
- Step 7** (Optional) Set up VM5 as Host Controller 2 for Service Catalog. For more information on how to set up Host Controller 2 for cluster nodes, see the instructions in [Adding Subsequent Host Nodes Manually in WildFly Cluster](#).
- Step 8** Install the Web Server.

Install the Apache web server, and configure it to point to the Cluster WildFly server group where RequestCenter.war was deployed. You must have a web server that acts as a load balancer on top of the cluster. All client connection to Service Catalog must go through the web server. Thus, the URL for Service Catalog will be

*[http://<web\\_server\\_host>:<web\\_server\\_port>/RequestCenter](http://<web_server_host>:<web_server_port>/RequestCenter)*

You can install the web server on its own VM, or if you'd like, you can install it on any of the existing VM because it won't interfere with the configuration of the other components that you have already installed in the previous steps.




---

**Note** Prime Service Catalog Installer does not install or configure the web server. You have to install the web server on your own. For configuring the Apache web server as a common web server for Service Catalog and Service Link, see [Setting Up Apache Web Server on WildFly](#).

---

If you selected the "Configure Windows Service" option during the installation, stop all the WildFly servers on VM1, VM3, VM4 and start them up again as windows services.

To stop the WildFly servers on these WildFly servers, open the Command Prompt window, where startServiceCatalogCluster.cmd is running, and press **Control-C** to stop the process and start the windows service called - **Cisco Prime Service Catalog**

- Step 9** (Optional) Add another node to the cluster.

If you want to add a third node to the cluster, repeat [Step 5](#) for setting up Node 3. After setting up Node 3, modify the Plugin settings for the web server that you set up in [Step 8](#), so that it is aware of the third cluster node.




---

**Note** You can execute the Prime Service Catalog Installer to add up to a 6th node to the cluster. If you want to add a 7th node or more, see section [Adding Subsequent Host Nodes Manually in WildFly Cluster](#).

---



**Next Step**

Proceed to setting up the domain controller node on VM1. See [Setting Up the Domain Controller Node \(VM 1\) in a Four VM Topology](#).

**Setting Up the Domain Controller Node (VM 1) in a Four VM Topology**

- 
- Step 1** On the machine designated for installing Domain Controller (in this case VM 1), launch the web interface installation wizard:
- On Windows Operating System, log in as a user with administrator rights and double-click `setup.cmd`.
  - On Linux Operating System, log in as the root user and execute `./setup.sh` from a graphical interface, such as X-window.
- Step 2** When the Introduction panel appears, click **Next** to begin.
- Step 3** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.
- On Windows, the default value for destination folder is `C:\CiscoPrimeServiceCatalog`.
  - On Linux, the default value is `/opt/CiscoPrimeServiceCatalog`. The value for destination directory must not contain any space character.

Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`.

For WildFly, this directory is also where the Service Catalog installer installs and configures the WildFly Application Server software.

- Step 4** On the Application Server Selection panel, select the application server as **WildFly** and click **Next**. The subsequent panels may look different depending on which application server you select at this point. Refer to the Application Server Information Worksheet that you filled out in Appendix A.
- Step 5** On the Setup Mode Selection panel, select **Cluster setup** radio button and click **Next**.
- Step 6** On the Node Type Selection panel, select the **Domain Controller Node** radio button and click **Next**. This option will install the Domain Controller on the VM 1.
- Step 7** On the Database Selection panel, select a database platform (Microsoft SQL Server or Oracle) and click **Next**. The subsequent panels may look different depending on which database platform you select at this point. Refer to the [Database Information Worksheet](#) that you filled out in Appendix A to determine your database platform.
- Step 8** On the Service Catalog Database Creation panel:
- If you have not created the database in advance, select **Yes**.  
By selecting **Yes**, you are telling the installer to create the database automatically for you. In the next panel, you will be prompted for the information that the installer will use to create the database user and database schema for Service Catalog. Refer to the [Database Information Worksheet](#) for the description of each field on this panel.
  - If you have already created your database or if you want to upgrade to an existing database, then select **No**.  
In the next panel, you will be prompted for the information of the existing database user and database schema. Refer to the [Database Information Worksheet](#) for the description of each field on this panel. (If you are performing an upgrade installation, you must select No. Refer to Chapter 7: [Upgrading Prime Service Catalog](#) for more detailed information).
- Step 9** On the Service Catalog Database panel, enter the information for the Service Catalog database.

- If you selected **Yes** in [Step 8](#), you will see a **Create Database** button on this panel, and the **Next** button is grayed out.

Notice that you need to enter the password for either the “sys” user (for Oracle) or the “sa” user (for SQL Server) which the installer will use to connect to your database server. Once you enter the information on this panel, click the **Create Database**. If you get the message “*Service Catalog database created successfully*,” click **OK** to close the message. The **Next** button is now enabled.

- If you selected **No** in [Step 8](#), you just need to fill out the information for the existing Service Catalog database, and select the **Execute database scripts** check box.




---

**Note** The “Create Database” feature creates a very basic Service Catalog database that meets the minimum requirements for the Service Catalog application to operate. This feature is recommended for a Demo or Test system. For a Production system, contact your DBA in advance, to create the Service Catalog database which meets all of the product requirements as described in the [Configuring Databases](#) section, as well as any performance, reliability, and security requirements that adhere to your corporate policy.

---

**Step 10** Click **Next** to continue. The installer connects to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if any database setting is missing. See the [Software Requirements](#) for the database requirements. If a database validation error occurs, you can do the following:

- Close the error dialog and click **Cancel** to exit the installation wizard.
- Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next panel.

**Step 11** In the Master Key Password panel, enter the master key password, if you selected **Yes** in step 8. Otherwise, enter the path to an existing KEK file that contains the Master Key Password for the existing database that you want to upgrade

As part of the security requirement, a master key password must be provided that would be used to encrypt all the passwords that are available in the application. The password provided must match the password rules, as described on the panel.

The master key password is saved in two files, `kek_new.txt` and `kek_old.txt`, under the `<ServiceCatalog_Install_Dir>/dist` directory. The `kek_new.txt` and `kek_old.txt` files must be backed up and stored in a safe location. The application server cannot login to the ServiceCatalog database without the master key password files. If you lose these master key password files, please contact Cisco TAC for help.

**Step 12** On Choose Java Virtual Machine panel, select the correct Java version for your platform. Click the **Search Another Location** button to navigate to the correct location of Java on your computer and click **Next**.




---

**Note** You must specify the location of Java for WildFly because the installer will install the WildFly Application Server software on your computer, and it will set the `JAVA_HOME` variable in the WildFly configuration to use this particular Java.

---

**Step 13** On the Domain Controller Configuration panel, enter the information for the WildFly server (IP address of this machine, i.e, VM 1). Refer to the [Service Catalog Configuration Table for WildFly](#) for the description of each field on this panel. Click **Next**.

- Step 14** On the Messaging Configuration panel, enter the information for the JMS Queue server (IP address of VM 2, where you will be installing Service Link next. This is also the IP address for JMS), and click **Next**. Refer to the [Messaging Configuration Table](#) for the description of each field on this panel.
- Remember the Queue password value that you would fill in the Messaging Configuration panel, as you need to enter same password when you install the Service Link later on VM 2.
- Step 15** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.
- Step 16** Click **Install** in the Preinstallation Summary panel to begin installation.
- The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.
- Step 17** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.
- Step 18** Start the Domain Controller and all managed servers on the Host 1.

**Note**

- For the first time after the installation, each WildFly server must be started as an application by executing the start script provided by Cisco, as also described in this step. **DO NOT** use the windows service called Cisco Prime Service Catalog to start the server.
- This start script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service.

To start the start the domain controller on Host 1, do the following:

- a. Access the `<ServiceCatalog_Install_Dir>\bin` directory.

```
cd <ServiceCatalog_Install_Dir>\bin
```

- b. Execute the following command to start the Domain Controller, Service Catalog, and Service Link:

[For Windows]:

```
startServiceCatalogCluster.cmd
```

[For Linux]

```
startServiceCatalogCluster.sh
```

- Step 19** Deploy RequestCenter.war. To deploy, do the following:

- a. Access the `<ServiceCatalog_Install_Dir>\bin` directory.

```
cd <ServiceCatalog_Install_Dir>\bin
```

- b. Execute the following command to the RequestCenter.war:

[For Windows]:

```
deployServiceCatalogCluster.cmd RC
```

[For Linux]

```
deployServiceCatalogCluster.sh RC
```

To stop the domain controller, execute the `stopDomainController` script. For information on the other scripts available with the installer for the standalone and cluster environment, see [WildFly Scripts](#).

### Next Steps

- Keep the following handy:
  - IP Address of VM 1 where the Domain Controller was installed.
  - Queue password that was set in the Messaging Configuration panel.
- Proceed to setting up the Service Link and JMS node on VM2. See [Setting Up the Service Link and JMS Node \(VM 2\) in a Four VM Topology](#).

## Setting Up the Service Link and JMS Node (VM 2) in a Four VM Topology

- 
- Step 1** Copy file “kek\_new.txt” from the `<ServiceCatalog_Install_Dir>/dist` directory on VM 1 to a temporary directory on VM 2.
- Step 2** Install Service Link and JMS node on VM2. Launch the web interface installation wizard.
- On Windows Operating System, log in as a user with administrator rights and double-click `setup.cmd`.
  - On Linux Operating System, log in as the root user and execute `./setup.sh` from a graphical interface, such as X-window.
- Step 3** When the Introduction panel appears, click **Next**.
- Step 4** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.
- On Windows, the default value for destination folder is `C:\CiscoPrimeServiceCatalog`.
  - On Linux, the default value is `/opt/CiscoPrimeServiceCatalog`. The value for destination directory must not contain any space character.
- Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`.
- Step 5** On the Application Server Selection panel, select the application server **WildFly** and click **Next**.
- Step 6** On the Setup Mode Selection panel, select **Standalone** radio button and click **Next**.
- Step 7** On the Installation Type panel, select **Custom** radio button and click **Next**.
- Step 8** On the Component Selection panel, select the **Service Link** radio button and click **Next**.
- Step 9** On the Database Selection panel, select a database platform (Microsoft SQL Server or Oracle) and click **Next**.
- Step 10** On the Service Catalog Database panel, enter the information for the Service Catalog database which was already created when you installed Domain Controller on VM 1, and click **Next** to continue.

The installer connects to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if any database setting is missing. See the [Software Requirements](#) for the database requirements. If a database validation error occurs, you can do the following:

- Close the error dialog and click **Cancel** to exit the installation wizard.
- Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next panel.

**Step 11** In the Master Key Password panel, enter the path to an existing KEK file (from [Step 1](#)) that contains the Master Key Password for the existing database.

As part of the security requirement, a master key password must be provided that would be used to encrypt all the passwords that are available in the application. The password provided must match the password rules, as described on the panel.

**Step 12** On Choose Java Virtual Machine panel, select the correct Java version for your platform. Click the **Search Another Location** button to navigate to the correct location of Java on your computer and click **Next**.



**Note** You must specify the location of Java for WildFly because the installer will install the WildFly Application Server software on your computer, and it will set the JAVA\_HOME variable in the WildFly configuration to use this particular Java.

**Step 13** On the Service Link Configuration panel, enter the following information:

- Enter the IP address of this VM in the **Service Link Host IP Address** field.
- Enter a password in the **WildFly admin password** field.
- Re-enter the same password in the **Confirm password** field.
- If the **Configure as windows service** option is displayed on the screen, select it.
- If the **Configure IIS** option is displayed on the screen, do NOT select it.

**Step 14** On the Messaging Configuration panel, enter the information for the JMS Queue server (IP address of this VM) where the Service Link will be deployed, and click **Next**. Refer to the [Messaging Configuration Table](#) for the description of each field on this panel. See the note below for the queue password field.



**Note** For the Queue password value, use the same password that you entered for “Queue password” during the installation of the Domain Controller on VM 1.

**Step 15** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.

**Step 16** Click **Install** in the Preinstallation Summary panel to begin installation.

The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.

**Step 17** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.

**Step 18** Start the Service Link server on the VM 2. This standalone WildFly server contains both the ServiceLink.war and the JMS service. To start the Service Link and JMS services, do the following:

- a. Access the `<ServiceCatalog_Install_Dir>\bin` directory.

```
cd <ServiceCatalog_Install_Dir>\bin
```

- b. Execute the following command to start the Domain Controller, Service Catalog, and Service Link:

[For Windows]:

```
startServiceLink.cmd
```

[For Linux]

```
startServiceLink.sh
```

On the Windows operating system, you can also start or stop the Service Link server, by starting or stopping the following Windows service:

### Cisco Prime Service Link

---

To stop the service link, execute the `stopServiceLink` script. For information on the other scripts available with the installer for the standalone and cluster environment, see [WildFly Scripts](#).

#### Next Steps

- Keep the following handy:
  - IP Address of VM 1 where the Domain Controller was installed.
  - IP address of VM 2, where the Service Link server and JMS were installed.
  - Queue password that was entered during the installation of the Domain Controller on VM 1.
- Proceed to setting up the VM3 and VM4 as Host Controller 1 and Host Controller 2 respectively. See [Setting Up Host Controller and Service Catalog For Cluster Nodes in a Four VM Topology](#).

### Setting Up Host Controller and Service Catalog For Cluster Nodes in a Four VM Topology

---

- Step 1** On the machine designated for Cluster Host 1, launch the web interface installation wizard:
- On Windows Operating System, log in as a user with administrator rights and double-click `setup.cmd`.
  - On Linux Operating System, log in as the root user and execute `./setup.sh` from a graphical interface, such as X-window.
- Step 2** When the Introduction panel appears, click **Next** to begin.
- Step 3** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.
- On Windows, the default value for destination folder is `C:\CiscoPrimeServiceCatalog`.
  - On Linux, the default value is `/opt/CiscoPrimeServiceCatalog`. The value for destination directory must not contain any space character.
- Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`.
- Step 4** On the Application Server Selection panel, select the application server as **WildFly** and click **Next**.
- Step 5** On the Setup Mode Selection panel, select **Cluster setup** radio button and click **Next**.
- Step 6** On the Node Type Selection panel, select **Host Controller Node** radio button and click **Next**.
- Step 7** On the Host Controller Selection panel, do the following:
- Choose **Host1** radio button if this machine should be set up as the first node of the cluster.
  - Choose **Host2** radio button if this machine should be set up as the second node of the cluster.



**Note** The Prime Service Catalog Installer will support only up to six nodes for the cluster. To add 7th node or more, please contact Cisco TAC.

---

- Step 8** Enter the Domain Controller IP Address to establish connection to the first machine (VM 1) where domain controller is installed.

**Step 9** On Choose Java Virtual Machine panel, select the correct Java version for your platform. Click the **Search Another Location** button to navigate to the correct location of Java on your computer and click **Next**.



**Note** You must specify the location of Java for WildFly because the installer will install the WildFly Application Server software on your computer, and it will set the JAVA\_HOME variable in the WildFly configuration to use this particular Java.

**Step 10** On the Service Catalog Configuration panel, enter the following information, and click **Next**:

- Service Catalog Host IP address: IP address of this machine, i.e., of the Cluster Host 1.
- In the Service Link URL field, enter `http://<SL_Address>:6080`, where `<SL_Address>` is the IP address of VM 2, where the Service Link server resides.
- If the “Configure as windows service” option is displayed on the screen, select it.

**Step 11** On the Messaging Configuration panel, enter the following information for the JMS Queue server, and click **Next**:

- Enter the IP address of VM 2 in the **Queue Host IP Address** field.
- In the **Queue password** field, enter the same password that you entered for **Queue password** during the installation of the Domain Controller on VM 1.

Refer to the [Messaging Configuration Table](#) for the description of each field on this panel.

**Step 12** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.

**Step 13** Click **Install** in the Preinstallation Summary panel to begin installation.

The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.

**Step 14** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.

**Step 15** Start the Host Controller for Cluster Host 1.



**Note**

- For the first time after the installation, each WildFly server must be started as an application by executing the start script provided by Cisco, as also described in this step. DO NOT use the windows service called Cisco Prime Service Catalog to start the server.
- This start script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service.

To start the Host Controller, do the following:

- Access the `<ServiceCatalog_Install_Dir>\bin` directory.

```
cd <ServiceCatalog_Install_Dir>\bin
```

- Execute the following command to start the Domain Controller, Service Catalog, and Service Link:  
[For Windows]:

```
startServiceCatalogCluster.cmd
```



[For Linux]

```
startServiceCatalogCluster.sh
```

The Host Controller will in turn, automatically start the managed server that belongs to the server group “main-server-group”. Since RequestCenter.war was already deployed in the “main-server-group” on the Domain Controller, it will also be automatically deployed onto this managed server.

**Step 16** Verify that you can connect to the following URL:

```
http://<VM3_or_VM4_IP_address>:8080/RequestCenter.
```

---

To stop the Host Controller and the Service Catalog server on both Host 1 and Host 2, execute the **forceStopAllOnHC** script. You can start and stop individual servers in a cluster. For information on the other start and stop scripts available with the installer for the WildFly cluster environment, see [WildFly Scripts](#).

#### Next Steps

Set up web server. See [Step 8 of Performing WildFly Cluster Installation for Four VM Topology](#).

## Postinstallation Tasks for WildFly

The Service Catalog installer installs and configures WildFly for the Service Catalog and Service Link services on your computer, but it will not automatically start up the WildFly service. This section contains instructions for starting and stopping the WildFly services for Service Catalog and Service Link and other postinstallation tasks for standalone and cluster WildFly setup.

## Postinstallation Tasks for WildFly Standalone Application Server

The following section includes the postinstallation tasks for standalone application server for WildFly.

### Enabling Secure Cookie

The secure cookie is an optional feature. To enable the secure cookie feature, you must first enable SSL for the web server, as you have already done in the "Preparing IIS Web Server" section. Then, after you install Prime Service Catalog, you must manually edit the file "`<PSC_Install_Dir>\WildFly-10.1.0.Final\ServiceCatalogServer\deployments\RequestCenter.war\WEB-INF\web.xml`" by setting the secure property to true as follows:

```
<session-config>
  <session-timeout>20</session-timeout>
<cookie-config>
  <http-only>true</http-only>
  <path>/RequestCenter</path>
  <secure>true</secure>
</cookie-config>
</session-config>
```



## Starting WildFly Server on Linux

Perform the following steps to start the WildFly Servers on Linux:

- 
- Step 1** It is assumed that your installation directory is "/opt/CiscoPrimeServiceCatalog". Use SSH to connect to the Linux machine as the "root" user, and navigate to the "/opt/CiscoPrimeServiceCatalog/bin" directory.
- Step 2** Execute the following command to start the WildFly server for Service Link in the background:  
**nohup ./startServiceLink.sh > startServiceLink.log 2>&1 &**
- Step 3** Wait for a few minutes for the Service Link server to be completely up. The JMS service is configured in the same WildFly server with the Service Link component application; thus, you want to allow enough time for the JMS service to be ready before starting up the Service Catalog application.
- Step 4** Execute the following command to start the WildFly server for Service Catalog in the background:  
**nohup ./startServiceCatalog.sh > startServiceCatalog.log 2>&1 &**
- Step 5** To stop the WildFly servers: It is recommended that you stop the Service Catalog application server first. Execute the following scripts as the "root" user to stop the WildFly servers for Service Catalog and Service Link:  
**./stopServiceCatalog.sh**  
**./stopServiceLink.sh**
- 

## Starting WildFly Server on Windows

If you selected the "Configure windows service" option for Service Catalog and Service Link during the installation, then the "Cisco Prime Service Catalog" service and "Cisco Prime Service Link" service are registered on your Windows Operating System.

However, the installer does not automatically start up the windows services for the first time right after the installation. (They will be automatically started the next time you reboot your computer.) You can perform the following steps to start the services for the first time:

- 
- Step 1** Select "*Start > All Programs > Administrative Tools > Services*" on your computer.
- Step 2** Do one of the following:
- Step 3** Select the service named **Cisco Prime Service Link**, and click the **Start Service** button.
- Step 4** Wait for a few minutes for the Service Link server to be completely up. The JMS service is configured in the same WildFly server with the Service Link component application; thus, you want to allow enough time for the JMS service to be ready before starting up the Service Catalog server.
- Step 5** Select the service named **Cisco Prime Service Catalog**, and click the **Start Service** button.
- 

To stop the WildFly servers: It is recommended that you stop the "Cisco Prime Service Catalog" service first, then stop the "Cisco Prime Service Link" service.

If you did not select the "Configure windows service" option during the installation, then you will need to execute a command script to start up each WildFly server. Perform the following steps to start the WildFly servers:

- 
- Step 1** It is assumed that your installation directory is "C:\CiscoPrimeServiceCatalog". Open a Command Prompt window, and navigate to the "C:\CiscoPrimeServiceCatalog\bin" directory.
- Step 2** Execute the script **startServiceLink.cmd** to start the WildFly server for Service Link.
- Step 3** Wait for a few minutes for the Service Link server to be completely up. The JMS service is configured in the same WildFly server with the Service Link component application; thus, you want to allow enough time for the JMS service to be ready before starting up the Service Catalog server.
- Step 4** Execute the script **startServiceCatalog.cmd** to start the WildFly server for Service Catalog.

**Note**

Because you start the WildFly servers using command scripts, if you log out of the Windows Operating System, the WildFly servers will be automatically killed when your login session is ended. So make sure that you don't log off the session where the WildFly servers are running. Follow the instructions in the "Configure WildFly As Windows Service" section below if you want to configure the WildFly servers as windows services after the installation. When the WildFly servers are running as windows services, they will not be killed when you log out of Windows Operating System.

- 
- Step 5** To stop the WildFly servers, you can either:
- Press Control+C in the Command Prompt window where the Service Link server or Service Catalog server is running, or
  - Execute the script "**stopServiceLink.cmd**" or "**stopServiceCatalog.cmd**", located under the C:\CiscoPrimeServiceCatalog\bin directory.
- 

## Configure WildFly as Windows Service

Perform the following steps to configure WildFly as Windows service:

- 
- Step 1** It is assumed that your installation directory is "C:\CiscoPrimeServiceCatalog". Open a Command Prompt window, and navigate to the "C:\CiscoPrimeServiceCatalog\bin" directory. Execute the script "**installServiceCatalogService.cmd**" to configure the WildFly server for Service Catalog as a Windows service. The service will be named "**Cisco Prime Service Catalog**".
- Step 2** Execute the script "**installServiceLinkService.cmd**" to configure the WildFly server for Service Link as a Windows service. The service will be named "**Cisco Prime Service Link**".
- Step 3** To remove the Windows services: First you need to manually stop the "Cisco Prime Service Catalog" and "**Cisco Prime Service Link**" services. Then, execute the scripts "**uninstallServiceCatalogService.cmd**" and "**uninstallServiceLinkService.cmd**".
- 

## Postinstallation Tasks for WildFly Clustered Application Servers

The following section includes the postinstallation tasks for clustered application servers for WildFly.

To start and stop individual servers in a cluster, see [WildFly Scripts](#) for information on the scripts available with the installer for the WildFly cluster environment.

**Note**

For WildFly cluster setup on Windows, keep the following in mind:

- For the first time after the installation, each WildFly server must be started as an application by executing the start script provided by Cisco. This script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service. Before starting the servers as windows service, you need to stop the servers, if they are already running with the help of the scripts provided by Cisco.
- When a WildFly server is started using the script provided by Cisco, the server runs in the foreground instead of background. As a result, if a user accidentally logs off from the machine where the WildFly server is running, the WildFly server process will be terminated.
- Because you start the WildFly servers using command scripts, if you log out of the Windows Operating System, the WildFly servers will be automatically killed when your login session is ended. So make sure that you don't log off the session where the WildFly servers are running. Follow the instructions in the "Configure WildFly As Windows Service" section below if you want to configure the WildFly servers as windows services after the installation. When the WildFly servers are running as windows services, they will not be killed when you log out of Windows Operating System.

## Configure WildFly as Windows Service

Perform the following steps to configure WildFly as Windows service:

- Step 1** It is assumed that your installation directory is "C:\CiscoPrimeServiceCatalog". Open a Command Prompt window, and navigate to the "C:\CiscoPrimeServiceCatalog\bin" directory. Execute the script "installProcessControllerClusterService.cmd" to configure the WildFly server for Cluster Service as a Windows service. The service will be named "Cisco Prime Service Catalog Cluster".
- Step 2** To remove the Windows services: First you need to manually stop the "Cisco Prime Service Catalog Cluster" and execute the script "uninstallServiceCatalogService.cmd".

## Setting Up Apache Web Server on WildFly

This section describes how to configure the httpd.conf file as a proxy server for the Service Catalog and Service Link servers. This procedure uses the "mod\_proxy" that comes with the installation of Apache (or Httpd) web server.

**Note**

The settings for Service Catalog differ for a clustered Wildfly deployment and a standalone Wildfly deployment.

### Procedure

- Step 1** Stop the Apache web server:
- ```
service httpd stop
```

**Step 2** Modify the httpd.conf file:

- a. If Service Catalog is deployed in clustered WildFly, replace the IP addresses in the httpd.conf file to the corresponding servers in your environment.

In the example below, replace the IP addresses in the httpd.conf, with the actual IP addresses of the following servers:

Web server's IP address = 10.78.0.100

Service Link's IP address = 10.78.0.200

Host 1 of Service Catalog's IP address = 10.78.0.300

Host 1 of Service Catalog's IP address = 10.78.0.400

```

ServerName 10.78.0.100

ServerRoot "/etc/httpd" Listen 80

Include conf.modules.d/*.conf
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so LoadModule
proxy_ftp_module modules/mod_proxy_ftp.so LoadModule proxy_http_module
modules/mod_proxy_http.so LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so LoadModule
proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so LoadModule
proxy_express_module modules/mod_proxy_express.so

User apache Group apache
ServerAdmin root@localhost

<Directory /> AllowOverride none Require all denied
</Directory>

DocumentRoot "/var/www/html"

#
# Relax access to content within /var/www.
#
<Directory "/var/www"> AllowOverride None
# Allow open access: Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html"> Options Indexes FollowSymLinks AllowOverride None
Require all granted
</Directory>

<IfModule dir_module> DirectoryIndex index.html
</IfModule>

<Files ".ht*"> Require all denied
</Files>

ErrorLog "logs/error_log" LogLevel warn

<IfModule log_config_module>
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common

<IfModule logio_module>
# You need to enable mod_logio.c to use %I and %O

```

```

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O"
combinedio
</IfModule>
CustomLog "logs/access_log" combined
</IfModule>

<IfModule alias_module>
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
</IfModule>

<Directory "/var/www/cgi-bin"> AllowOverride None Options None
Require all granted
</Directory>

<IfModule mime_module> TypesConfig /etc/mime.types AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
AddType text/html .shtml AddOutputFilter INCLUDES .shtml
</IfModule> AddDefaultCharset UTF-8
<IfModule mime_magic_module> MIMEMagicFile conf/magic
</IfModule> EnableSendfile on
IncludeOptional conf.d/*.conf

<VirtualHost *:80>

ServerName 10.78.0.100
ProxyRequests Off
ProxyPreserveHost On
ProxyTimeout 1200
LimitRequestFieldSize 65536
ProxyIOBufferSize 65536

<Location ~ "/IntegrationServer">
ProxyPass "http://10.78.0.200:6080/IntegrationServer" Order allow,deny
Allow from all
</Location>

<Location /balancer-manager> SetHandler balancer-manager Order allow,deny
Allow from all
</Location>

Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e; path=/"
env=BALANCER_ROUTE_CHANGED

<Proxy balancer://mycluster>
BalancerMember http://10.78.0.300:8080 route=1 BalancerMember http://10.78.0.400:8080
route=2 ProxySet stickysession=ROUTEID
</Proxy>

ProxyPass / balancer://mycluster/ ProxyPassReverse / balancer://mycluster/

</VirtualHost>

```

- b. If the Service Catalog is deployed in standalone WildFly, replace the IP addresses in the `httpd.conf` file to the corresponding servers in your environment.

In the example below, it is assumed that Service Catalog and Service Link servers reside on the same VM. Replace the IP addresses, with the actual IP addresses of the corresponding servers in your environment:

Web server's IP address = 10.78.0.100

Service Link's IP address = 10.78.0.200

Service Catalog's IP address = 10.78.0.200

Everything in `httpd.conf` is the same as in 2a) above, except for the `<VirtualHost>` section at the end:

```
<VirtualHost *:80>

ServerName 10.78.0.100 ProxyRequests Off ProxyPreserveHost On

<Location ~ "/IntegrationServer">
ProxyPass "http://10.78.0.200:6080/IntegrationServer" Order allow,deny
Allow from all
</Location>

<Location ~ "/RequestCenter">
ProxyPass "http://10.78.0.200:8080/RequestCenter" Order allow,deny
Allow from all
</Location>

</VirtualHost>
```

**Step 3** To connect the server to a specific port (for ex:8080), run the below command:

```
semanage port -?a -?t http_port_t -?p tcp 8080
```

**Step 4** To allow the server to access the different IP's and ports defined in the load balancer settings, execute the below command:

```
setsebool -?P httpd_can_network_connect 1
```

**Step 5** Start the Apache web server, using the below command:

```
service httpd start
```

## Enabling SSL on Apache Web Server and IIS Server

If you need Prime Service Catalog to be accessed securely, configure the existing virtual host for SSL on Apache web server as described below.

### Standalone mode:

In the `standalone_full.xml` file, modify scheme value to "https".

```
"<ajp-listener name="ajp" socket-binding="ajp" scheme="https" max-ajp-packet-size=65536/>"
```

### Cluster mode:

In the `domain.xml` file, modify scheme value to "https" for both RC and service link nodes.

Example:

```
"<ajp-listener name="ajp" socket-binding="ajp" scheme="https" max-ajp-packet-size=65536/>"
```

## Applying Patch or Customizations to the WildFly Cluster Setup

- [For 2 VM Cluster Topology](#)
- [For 4 VM Cluster Topology](#)

### For 2 VM Cluster Topology

Perform the following steps on a two VM for applying a patch or any customizations.



#### Note

This procedure is based on the assumption that all servers are still running on both VM1 and VM2 for 2 VM topology.

**Step 1** Login to VM1 and access the <ServiceCatalog\_Install\_Dir>\bin directory.

**Step 2** Undeploy the .war file:

- Remove the RequestCenter.war and ISEE.war from all the host controllers, by executing the following command:

```
undeployServiceCatalogCluster.cmd ALL
```

- If you want to undeploy just RequestCenter.war, then execute the following command:

```
undeployServiceCatalogCluster.cmd RC
```

- if you want to undeploy just ISEE.war, then execute the following command:

```
undeployServiceCatalogCluster.cmd SL
```

**Step 3** Shutdown all the servers by executing the following commands on VM1:

```
shutdownAllOnHC2.cmd  
shutdownAllOnHC1.cmd
```

**Step 4** Backup the original dist/RequestCenter.war and dist/ISEE.war, if you plan to change it. To do so, execute the following command:

```
md temp_dir\RequestCenter.war  
md temp_dir\ISEE.war
```

**Step 5** Extract the appropriate WAR file(s) that you want to customize:

- Extract the original dist/RequestCenter.war to a temporary directory, such as /temp/RequestCenter.war by executing the following command:

```
cd temp_dir\RequestCenter.war  
jar xvf <ServiceCatalog_Install_Dir>\dist\RequestCenter.war > nul
```

- Extract the original dist/ISEE.war to a temporary directory, such as /temp/ISEE.war

```
cd temp_dir\ISEE.war  
jar xvf <ServiceCatalog_Install_Dir>\dist\ISEE.war > nul
```

**Step 6** Apply the customizations:

- Apply the customizations by modifying or overwriting the files in the /temp\_dir/RequestCenter.war directory.
- Apply the customization by modifying or overwriting the files in the /temp\_dir/ISEE.war directory.

**Step 7** Zip up the RequestCenter.war file and ISEE.war file:

- a. To zip up the /temp\_dir/RequestCenter.war directory into a RequestCenter.war file, execute the following commands:

```
cd temp_dir\RequestCenter.war
jar -cvf RequestCenter.war.\META-INF\MANIFEST.MF *
```

A compressed version of RequestCenter.war is created in temp\_dir\RequestCenter.war.

- b. To zip up the /temp\_dir/ISEE.war directory into a ISEE.war file, execute the following commands:

```
cd temp_dir\ISEE.war
jar -cvf ISEE.war.\META-INF\MANIFEST.MF *
```

A compressed version of ISEE.war is created in temp\_dir\ ISEE.war.

**Step 8** Overwrite the new versions of the war files in the "dist" directory:

- a. Copy the new version of RequestCenter.war into the <ServiceCatalog\_Install\_Dir>\dist directory, overwriting the existing file.
- b. Copy the new version of ISEE.war into the <ServiceCatalog\_Install\_Dir>\dist directory, overwriting the existing file.

**Step 9** Delete the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/content directory on VM1.

**Step 10** Remove the domain/servers/<servername>/tmp/\* on VM1:

- a. Delete everything under <ServiceCatalog\_Install\_Dir>/wildfly-10.1.010.1.0.Final/domain/servers/server-host1-RC/tmp directory.
- b. Delete everything under <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/domain/servers/server-host1-SL/tmp directory.

**Step 11** Start the servers on VM1. To do this execute the following commands on VM1.

```
startServiceCatalogCluster.cmd
```

**Step 12** Deploy the latest war files on VM1:

- To deploy the latest version of RequestCenter.war followed by ISEE.war, execute the following command:

```
deployServiceCatalogCluster.cmd ALL
```

- To deploy just RequestCenter.war, execute the following command:

```
deployServiceCatalogCluster RC
```

- To deploy just ISEE.war, execute the following command:

```
deployServiceCatalogCluster SL
```

**Step 13** On VM2, do the following:

- a. Copy the new version of RequestCenter.war on VM1 into the <ServiceCatalog\_Install\_Dir>\dist directory on VM2, overwriting the existing file on VM2.
- b. Login to VM2.
- c. Delete the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/content directory on VM2.
- d. Delete everything under the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/domain/servers/server-host2-RC/tmp directory.
- e. Start all the servers on VM2 by executing the following command:



```
startServiceCatalogCluster.cmd
```

This script will automatically recreate the missing  
<ServiceCatalog\_Install\_Dircontent/content/RequestCenter.war directory on this VM.



**Note** After applying the patch, each WildFly server must be started as an application by executing the start script provided by Cisco. This script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service. Before starting the servers as windows service, you need to stop the servers, if they are already running with the help of the scripts provided by Cisco.

### For 4 VM Cluster Topology

Perform the following steps on a four VM topology for applying a patch or any customizations.



**Note** This procedure is based on the assumption that all servers are still running on both VM1, VM3, and VM4 for a 4 VM topology.

- Step 1** Login to VM1 and access the <ServiceCatalog\_Install\_Dir>\bin directory.
- Step 2** Remove the RequestCenter.war from all the Host Controllers by executing the following command on VM1:
- ```
undeployServiceCatalogCluster.cmd RC
```
- Step 3** Stop all the servers on VM3 by executing the following command on VM1:
- ```
shutdownAllOnHC1.cmd
```
- Step 4** Stop all the servers on VM4 by executing the following command on VM1:
- ```
shutdownAllOnHC2.cmd
```
- Step 5** Backup the original dist/RequestCenter.war file. To do so, execute the following command:
- ```
md temp_dir\RequestCenter.war
```
- Step 6** Extract the original dist/RequestCenter.war to a temporary directory, such as /temp/RequestCenter.war. To do so, execute the following command:
- ```
cd temp_dir\RequestCenter.war
jar xvf <ServiceCatalog_Install_Dir>\dist\RequestCenter.war > nul
```
- Step 7** On VM1, apply the customizations by modifying or overwriting the files in the /temp\_dir/RequestCenter.war directory.
- Step 8** Zip up the /temp\_dir/RequestCenter.war directory into a RequestCenter.war file as follows:
- ```
cd temp_dir\RequestCenter.war
jar -cvf RequestCenter.war .\META-INF\MANIFEST.MF *
```
- A compressed version of RequestCenter.war is created in temp\_dir\RequestCenter.war.
- Step 9** Copy the new version of RequestCenter.war into the <ServiceCatalog\_Install\_Dir>\dist directory, overwriting the existing file.

**Step 10** On VM1, deploy the latest version of RequestCenter.war in all host controllers. To do this execute the following commands on VM1.

```
deployServiceCatalogCluster.cmd RC
```

**Step 11** On VM2 (Service Link Server), apply the customization in the ISEE.war directory by doing the following:

a. Login to VM2.

b. Stop the Service Link Server by executing the following command:

```
stopServiceLink.cmd
```

c. Backup

<ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/ServiceLinkServer/deployments/ISEE.war directory to a temporary directory. To do so, execute the following command:

```
md temp_dir\ISEE.war
cd temp_dir\ISEE.war
jar xvf <ServiceCatalog_Install_Dir>\ServiceLinkServer\deployments\ISEE.war > nul
```

d. Apply the customization directly in the <ServiceCatalog\_Install\_Dir>\ServiceLinkServer\deployments\ISEE.war directory.

e. Delete everything under the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/ServiceLinkServer/tmp directory.

f. Start the Service Link server by executing the following command:

```
startServiceLink.cmd
```

**Step 12** Copy new version of RequestCenter.war from <ServiceCatalog\_Install\_Dir>\dist directory on VM 1 to the <ServiceCatalog\_Install\_Dir>\dist directory, overwriting the existing file on VM3 and VM4.

**Step 13** Log in to VM3.

**Step 14** Delete the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/content directory.

**Step 15** Delete everything under the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/domain/servers/server-host1-RC/tmp directory.

**Step 16** Start all the servers on VM3 by executing the following script:

```
startServiceCatalogCluster.cmd
```

**Step 17** Log in to VM4.

**Step 18** Delete the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/content directory.

**Step 19** Delete everything under the <ServiceCatalog\_Install\_Dir>/wildfly-10.1.0.Final/domain/servers/server-host2-RC/tmp directory.

**Step 20** Start all the servers on VM3 by executing the following script:

```
startServiceCatalogCluster.cmd
```

This script will automatically recreate the missing `<ServiceCatalog_Install_Dir/content/*.war` directory on both VM3 and VM4.



**Note** After applying the patch, each WildFly server must be started as an application by executing the start script provided by Cisco. This script will create the content folder and generate necessary files in the installation directory. After this is done, then from the next time you can directly start the servers as windows service. Before starting the servers as windows service, you need to stop the servers, if they are already running with the help of the scripts provided by Cisco.

When both Request Center and Service Link applications are deployed, they are in preparation state, they must be moved to Active state by starting them in following order:

First start Service Link. Only after Service Link is in the Active state, start RequestCenter. Make sure it is in active state before you try verifying the installation.

## Verifying Your Installation

Verify your installation by performing the following tasks:

- Step 1** Open a browser, and connect to the following URL: <http://<hostname>:<port>/RequestCenter> where
- `<hostname>` = The fully qualified domain hostname or the IP address of the computer where you installed the WildFly server for Service Catalog.
  - `<port>` =The HTTP Port number assigned to the Wildfly server for Service Catalog. The default value for HTTP Port number is 8080.



**Note** If you are on a Windows Operating System, and during the installation you selected the "Configure IIS" option, then the Service Catalog installer automatically configured the tomcat plugin for the IIS web server on your machine to redirect to the WildFly server. Thus, in this case, the URL for Service Catalog should point to the port number used by the IIS web server instead. For example, if your IIS web server is using port 80, then the URL should be `http://<hostname>:80/RequestCenter`, or `http://<hostname>/RequestCenter` since port 80 can be omitted from the URL.

- Step 2** Log in as the Site Administrator. For a new installation of Service Catalog, the username for the Site Administrator is "admin" and the password is the value you entered on the Service Catalog Administration Configuration panel of the installation wizard.
- Step 3** Navigate to the Service Link module.
- Step 4** On the left hand side of the panel, under Service Link Status, verify that the connection has a green status.

You have completed the installation for Cisco Prime Service Catalog on WildFly.





# Setting Up WebLogic Application Server

If you choose WebLogic as your application server, you need to install the Oracle WebLogic Application Server software as a prerequisite on your machine. This guide does not contain instructions for installing the WebLogic software. However, you will need to follow the instructions in the Preinstallation Configuration for WebLogic to prepare your WebLogic Server for use with Service Catalog. Then after you execute the Cisco Prime Service Catalog installer, come back to the Postinstallation Configuration for WebLogic section of this chapter to complete the rest of the configuration steps.

## Preinstallation Configuration for WebLogic

This section contains instructions for configuring the Oracle WebLogic Application Server, prior to installing Prime Service Catalog.

This release of Prime Service Catalog supports the WebLogic Application Server on the following Operating Systems and Java Development Kit:

**Table 5-1 Supported Operating Systems and Java**

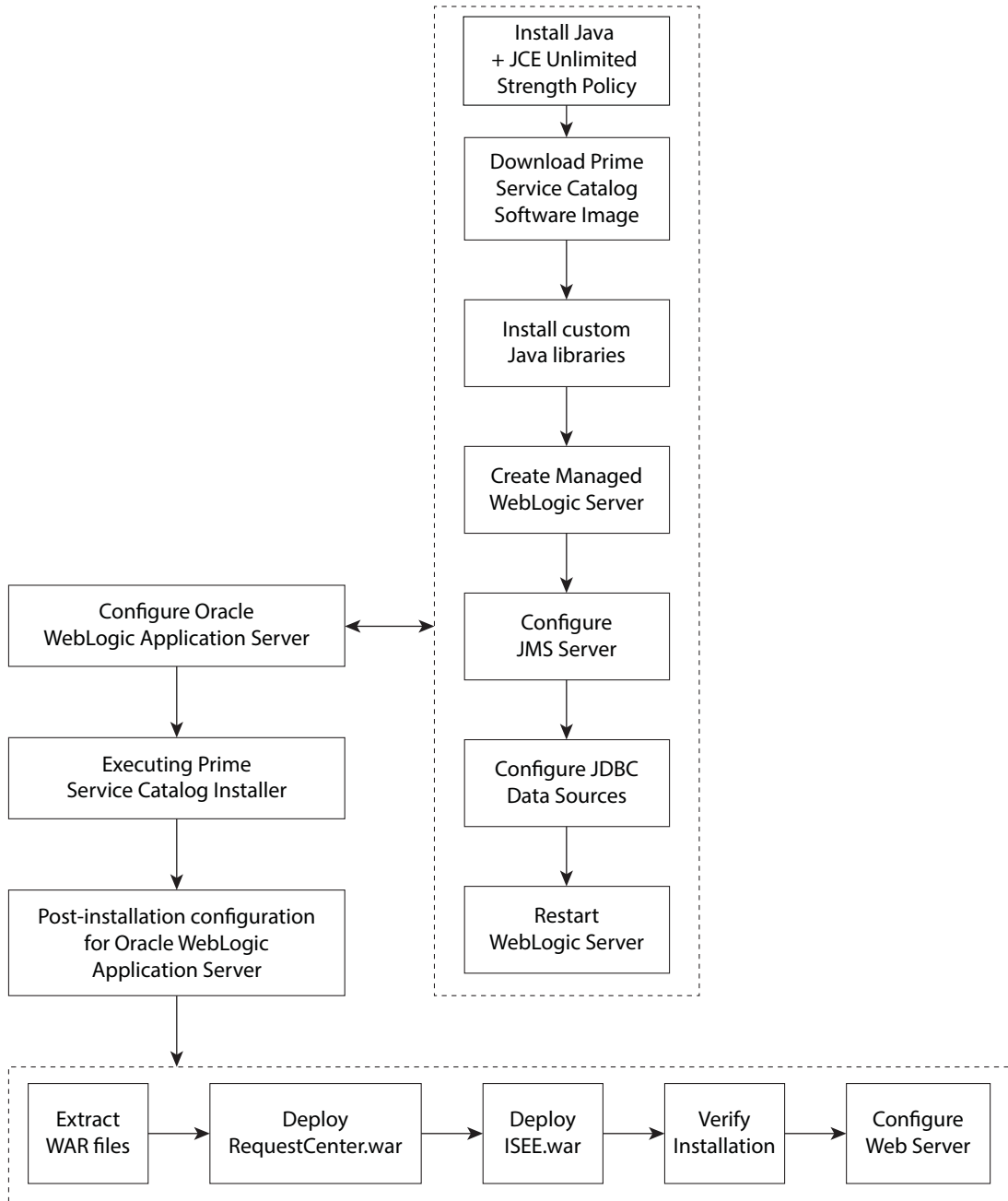
<b>Oracle WebLogic Application Server</b>	<b>Operating System</b>	<b>Java</b>
Version 12c (12.2.1.2)	Red Hat Enterprise Linux Server 7.3	Oracle JDK 8 Update 91(or higher update)
Version 12c (12.2.1.2)	Windows Server 2012 R2	Oracle JDK 8 Update 91 (or higher update)

It is assumed that you have already installed WebLogic Server 12c (12.2.1.2) software on one of the supported Operating Systems. You will follow instructions in this section to create and configure a new managed WebLogic Server, exclusively for the Cisco Prime Service Catalog application.

# WebLogic Installation Flow

The following figure illustrates steps to install Prime Service Catalog on Oracle WebLogic Application Server.

**Figure 5-1** Installation Flow for Oracle WebLogic Application Server



364205

## Installing Java

Although the WebLogic software installation is bundled with some version of JRockit or Oracle Java, you will not use any bundled JRockit or Java. Instead, you need to download and install Oracle JDK 8. In the next section, you will configure your WebLogic Server to use this version of Oracle JDK 8. This section needs to be done regardless of whether you install WebLogic Server on Windows operating system or Linux operating system.

**Note**

Currently Prime Service Catalog supports IPv4 only. Ensure that IPV6 is disabled on the installation box.

- 
- Step 1** Access the Oracle JDK 8 download web site to download Oracle JDK 8.
  - Step 2** Download the correct version of Oracle JDK 8 for your OS platform. See [Table 5-1](#) for the supported Update version of JDK 8.
  - Step 3** Install Oracle JDK 8 on the same machine where WebLogic software is installed.
  - Step 4** Set \$JAVA\_HOME and add JAVA\_HOME to PATH.
  - Step 5** Copy the unlimited strength JCE policy files to the \$JAVA\_HOME/jre/lib/security directory, overwriting the existing files. The unlimited strength policy files are "local\_policy.jar" and "US\_export\_policy.jar", which can be downloaded from the following link:  
<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>
  - Step 6** Restart all WebLogic servers, including the WebLogic Administration Server and Node Manager.

**Note**

If you have a WebLogic Cluster environment, perform Steps 3–5 on every node in the Cluster.

## Downloading Prime Service Catalog Software

You must first download the Prime Service Catalog software prior to proceeding to the Installing Custom Java Libraries step. For details about the software image download, see [Downloading Prime Service Catalog Software Image](#).

## Installing Custom Java Libraries

In this section, you will copy several Java library files from the `<ServiceCatalog_Software_Dir>` to the `<WL_HOME>` directory, and add these jar files to the class paths. Afterward, you need to restart the WebLogic servers in order to pick up the new Java libraries. This procedure remains same for Windows and Linux platforms.

- 
- Step 1** Under the "`<WL_HOME>`" directory, create a subdirectory called "**lib**".
  - Step 2** Copy the following jar files from the "`<ServiceCatalog_Software_Dir>\preinstall\weblogic\cisco_lib`" directory to the "`<WL_HOME>\user_projects\domains\<yourdomain>\lib`" directory:

- bcprov-jdk15on-1.50.jar
- ojdbc7.jar
- pluto-container-2.0.2.jar
- pluto-container-api-2.0.2.jar
- pluto-container-driver-api-2.0.2.jar
- pluto-portal-driver-api-2.0.2.jar
- pluto-portal-driver-impl-2.0.2.jar
- pluto-taglib-2.0.2.jar
- portlet-api\_2.0\_spec-1.0.jar
- sqljdbc4.jar

**Step 3** Restart the WebLogic Administration Server and WebLogic Node Manager. You must restart all WebLogic servers for them to pick up the custom Java libraries that you just installed.




---

**Note** If you have a WebLogic Cluster environment, repeat this procedure on every node in the Cluster.

---




---

**Note** If you are upgrading from a previous release of Prime Service Catalog to this release, you must still perform this procedure in this section on your WebLogic environment. This is because:

- a) You have to overwrite the older version of the Cisco jar files with the newer version shipped with this release of Prime Service Catalog.
- b) There are new version of JDBC drivers that are bundled with this release of Prime Service Catalog.
- c) Ensure to point the JAVA\_HOME to JDK 1.8 version.

---

## Creating a Managed WebLogic Server

In this section you will create a new managed WebLogic Server, to be used exclusively for Prime Service Catalog.

- 
- Step 1** Log on to the WebLogic Administration Console.
- Step 2** If your WebLogic was installed in PRODUCTION mode, click **Lock & Edit** so that you can proceed to make changes. Otherwise, you can skip this step.
- Step 3** Choose **Environment > Servers**.
- Step 4** Click **New**. The “Create a New Server” panel appears.



Figure 5-2 Create New WebLogic Server

**Create a New Server**

Back Next Finish Cancel

**Server Properties**

The following properties will be used to identify your new server.  
\* Indicates required fields

What would you like to name your new server?

\* **Server Name:**

Where will this server listen for incoming connections?

**Server Listen Address:**

\* **Server Listen Port:**

Should this server belong to a cluster?

**No, this is a stand-alone server.**

**Yes, create a new cluster for this server.**

Back Next Finish Cancel

361938

- Step 5** Enter a Server Name (for example, “server1”). Enter a port number different from 7001 (for example, 8001), because port 7001 is most likely already used by the WebLogic Administration Server. Choose the **No, this is a stand-alone server** option.
- Step 6** Click **Finish**. Your newly created WebLogic Server appears on the list.
- Step 7** Click the newly created Server “**server1**” to open its properties.
- Step 8** Choose **Configuration > General**.

Figure 5-3 Configuration – General Settings

Settings for server1

Configuration Protocols Logging Debug Monitoring Control Deployments Serv

General Cluster Services Keystores SSL Federation Services Deployment Mig

Save

Use this page to configure general features of this server such as default network communicat

[View JNDI Tree](#)

**Name:** server1

**Machine:** vmsw06.oakqas.celosis.com

**Cluster:** (Stand-Alone)

**Listen Address:**

**Listen Port Enabled**

**Listen Port:**

**SSL Listen Port Enabled**

361939

- Step 9** In the Machine drop-down list, select a machine (i.e. Node Manager machine) where the WebLogic server will run, and click **Save**.
- Step 10** Choose **Configuration > Keystores**.
- Step 11** Click the **Change** button next to the **Keystores** field. Select **Custom Identity and Java Standard Trust** from the drop-down list. Click **Save**.

## Setting the Arguments for Java Virtual Machine

Perform the following steps to set the arguments for Java Virtual Machine:

**Step 1** Choose **Configuration > Server Start**.

**Step 2** Enter values for the following parameters:

- **Arguments =**

**For Request Center:** -server -Xms4096m -Xmx4096m -XX:NewRatio=1  
 -XX:ReservedCodeCacheSize=256m -XX:+TieredCompilation  
 -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/tmp  
 -Dweblogic.http.enableRemoteUserHeader=true  
 -XX:CompileCommand=exclude,com/newscaler/bfw/signon/filters/AuthenticationFilter,doFilter  
 -XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement  
 -XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal  
 -XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr  
 -XX:CompileCommand=exclude,org/apache/oro/text/regex/Perl5Compiler,\_\_parseAtom  
 -XX:+PrintGCDetails -Xloggc:/tmp/WL12c\_RC\_Baseline.log  
 -XX:+PrintGCTimeStampsUser

**For Service Link:** -server -Xms2048m -Xmx2048m -XX:NewRatio=1  
 -XX:ReservedCodeCacheSize=256m -XX:+TieredCompilation  
 -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/tmp  
 -Dweblogic.http.enableRemoteUserHeader=true  
 -XX:CompileCommand=exclude,com/newscaler/bfw/signon/filters/AuthenticationFilter,doFilter  
 -XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement  
 -XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal  
 -XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr  
 -XX:CompileCommand=exclude,org/apache/oro/text/regex/Perl5Compiler,\_\_parseAtom  
 -XX:+PrintGCDetails -Xloggc:/tmp/WL12c\_SL\_Baseline.log -XX:+PrintGCTimeStamps

Where, -Xloggc:/tmp/WL12c\_SL\_Baseline.log is for Linux and  
 -Xloggc:c:\WL12c\_SL\_Baseline.log is for Windows.

- **Name** = weblogic
- **Password** = <the password for the “weblogic” username>
- **Confirm Password** = <re-enter the password for the “weblogic” username>

**Step 3** Click **Save**.

**Step 4** If your WebLogic was installed in PRODUCTION mode, click **Activate Changes**. Otherwise, you can skip this step.

**Step 5** Open the **Control** tab.

Figure 5-4 Start WebLogic Server

Servers(Filtered - More Columns Exist)

Start Resume Suspend Shutdown Restart SSL Showing 1 to 2 of 2 Previous | Next

<input type="checkbox"/>	Server	Machine	State	Status of Last Action
<input type="checkbox"/>	AdminServer(admin)		RUNNING	None
<input checked="" type="checkbox"/>	server1	vmmsw06.oakqas.celosis.com	RUNNING	TASK COMPLETED

361940

- Step 6** Choose the WebLogic Server named “**server1**”, then click **Start**. Wait until you see State=RUNNING. Your new WebLogic Server has now been configured to use Oracle JDK 8 and the Cisco Java libraries that you installed in this section.

## WebLogic Cluster Configuration

The Prime Service Catalog product is comprised of two component applications named “Service Catalog” and “Service Link”. However, the Prime Service Catalog installer does not automatically deploy the Service Catalog and Service Link applications on your WebLogic Server for you. The installer will generate two WAR files (RequestCenter.war for the Service Catalog component application, and ISEE.war for the Service Link component application) which are customized for your WebLogic environment. After you execute the Prime Service Catalog installer, you will need to follow the instructions in a later section of this chapter to manually deploy RequestCenter.war and ISEE.war on your WebLogic Server.

The RequestCenter.war file and ISEE.war file can be deployed together in the same WebLogic Server even though they are two separate component applications. However, if you are setting up a WebLogic Cluster environment with multiple nodes (where each node is a separate computer), you need to perform the additional configurations as follows:

- Step 1** Perform the tasks described in the [Installing Java](#) and [Installing Custom Java Libraries](#) on each node (that is, each computer) in the Cluster.
- Step 2** Follow the instructions in the [Creating a Managed WebLogic Server](#) to create the WebLogic Server for each node and to set the JVM arguments for each server, before you add these servers to the Cluster.
- Step 3** Each WebLogic Server in your Cluster must be configured to use the same port number. For example, your Cluster contains two nodes. If the WebLogic Server on Host 1 is running on port 8001, then the WebLogic Server on Host 2 must also be configured to run on port 8001.
- Step 4** RequestCenter.war file is deployed on the WebLogic Cluster. But, the ISEE.war file cannot be deployed in the same Cluster; it must be deployed on a stand-alone WebLogic Server that is not a member of any Cluster. Therefore, if you have a clustered WebLogic environment, then you must create an additional stand-alone WebLogic Server (that is, not a member of the Cluster), to be used for ISEE.war. For the rest of the chapter, this stand-alone WebLogic Server is referred to as the “Service Link WebLogic Server”. For this stand-alone “Service Link WebLogic Server”, the JVM arguments can be set as follows:

```
-server -Xms2048m -Xmx2048m -XX:NewRatio=1 -XX:ReservedCodeCacheSize=256m
-XX:+TieredCompilation -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/tmp
-Dweblogic.http.enableRemoteUserHeader=true
-XX:CompileCommand=exclude,com/newscale/bfw/signon/filters/AuthenticationFilter,doFilter
-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement
```

```
-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal
-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr
-XX:CompileCommand=exclude,org/apache/oro/text/regex/Perl5Compiler,__parseAtom
-XX:+PrintGCDetails -Xloggc:/tmp/WL12c_SL_Baseline.log -XX:+PrintGCTimeStamps
```

- Step 5** If the stand-alone “Service Link WebLogic Server” resides on another machine, then make sure that you also performed the tasks described in the [Installing Java](#) and [Installing Custom Java Libraries](#) on that WebLogic machine. If the stand-alone “Service Link WebLogic Server” resides on the same machine as one of the Cluster nodes, then make sure that it is configured with a port number that is different from the port number used by the Cluster.

## Configuring JMS Server

In this section, you will configure a JMS Server and JMS Queues that will be used by Prime Service Catalog.



### Note

If RequestCenter.war and ISEE.war are deployed together on the standalone or cluster WebLogic Server, then the JMS configurations described in this section are performed for the “Service Link WebLogic Server”.

## Creating a Persistent Store

Perform the following steps to create a persistent store:

- Step 1** On your computer, cd to `<WL_HOME>`.
- Step 2** Create a subdirectory called **CiscoFileStore**.
- Step 3** Log on to the WebLogic Administration Console.
- Step 4** If your WebLogic was installed in PRODUCTION mode, click **Lock & Edit**. Otherwise, you can skip this step.
- Step 5** Choose **Services > Persistent Stores**.
- Step 6** Choose **New > Create FileStore**. The “Create a New File Store” panel appears.
- Step 7** In the Name field, enter **CiscoFileStore**.
- Step 8** In the Target drop-down list, choose your WebLogic Server.
- Step 9** In the Directory text box, enter the full path of the CiscoFileStore directory you created in Step 2 above (for example, `/opt/Oracle/Middleware/wlserver_10.3/CiscoFileStore`).
- Step 10** Click **OK**.

## Creating a JMS Server

Perform the following steps to create JMS server:

- Step 1** On the WebLogic Administration Console, choose **Services > Messaging > JMS Modules**.

- Step 2** Click **New**. The “Create a New JMS Server” panel appears.
  - Step 3** In the Name field, enter **CiscoJMSServer**.
  - Step 4** In the Persistent Store drop-down list, choose the Persistent Store named **CiscoFileStore**.
  - Step 5** Click **Next**.
  - Step 6** In the Target drop-down list, choose your WebLogic Server. (If you have a WebLogic Cluster environment, click **Service Link WebLogic Server**.)
  - Step 7** Click **Finish**.
- 

## Creating a JMS Module

Perform the following steps to create a JMS module:

- Step 1** On the WebLogic Administration Console, choose **Services > Messaging > JMS Modules**.
  - Step 2** Click **New**. The Create JMS System Module panel appears.
  - Step 3** In the Name field, enter **CiscoJMSModule**. and click **Next**.
  - Step 4** Choose your WebLogic Server as the target. (If you have a WebLogic Cluster environment, choose **Service Link WebLogic Server**.) and click **Next**.
  - Step 5** Click **Finish**.
  - Step 6** Click the newly created JMS Module named **CiscoJMSModule** to open its properties.
  - Step 7** Open the **Subdeployments** tab and click **New**.
  - Step 8** In the Subdeployment Name field, enter **CiscoSubdeployment** and click **Next**.
  - Step 9** Choose the JMS Server named **CiscoJMSServer**. and click **Finish**.
- 

## Creating Connection Factory

Perform the following steps to create a connection factory:

- Step 1** On the WebLogic Administration Console, choose **Services > Messaging > JMS Modules**.
- Step 2** Click the JMS Module named **CiscoJMSModule** to open its properties.
- Step 3** Open the **Configuration** tab and click **New**.
- Step 4** Choose the **Connection Factory** option and click **Next**.
- Step 5** In the Name and JNDI Name fields, enter **NSConnectionFactory** and click **Next**.



**Note** Make a note of the *NSConnectionFactory* value as it will be used during the Prime Service Catalog.

---

- Step 6** Click **Advanced Targeting**.
- Step 7** In the Subdeployments drop-down list, choose **CiscoSubdeployment**. The screen is refreshed to show that the JMS Server named “CiscoJMSServer” is already selected.

**Step 8** Click **Finish**.

---

## Creating JMS Templates

Perform the following steps to create JMS templates:

- 
- Step 1** On the WebLogic Administration Console, choose **Services > Messaging > JMS Modules**.
  - Step 2** Click the JMS Module named **CiscoJMSModule** to open its properties.
  - Step 3** Open the **Configuration** tab and click **New**.
  - Step 4** Choose the **JMS Template** option and click **Next**.
  - Step 5** In the Name field, enter **CiscoQueueTemplate** and click **OK**.
- 

## Creating Queues

Perform the following steps to create queues:

- 
- Step 1** On the WebLogic Administration Console, choose **Services > Messaging > JMS Modules**.
  - Step 2** Click the JMS Module named **CiscoJMSModule** to open its properties.
  - Step 3** Open the **Configuration** tab and click **New**.
  - Step 4** Choose the **Queue** option.
  - Step 5** Click **Next**.
  - Step 6** In the Name and JNDI Name fields, enter **ISEEInboundQueue**.
  - Step 7** In the Template drop-down list, choose the **CiscoQueueTemplate** that you created and click **Next**.
  - Step 8** In the Subdeployments drop-down list, choose **CiscoSubdeployment**. The screen is refreshed to show that the JMS Server named “CiscoJMSServer” is already selected.
  - Step 9** Click **Finish**.
  - Step 10** Repeat the above steps four more times to create four more JMS Queues with the following names:

<b>Name &amp; JNDI Name</b>	<b>Template</b>	<b>Subdeployments</b>
ISEEOutboundQueue	CiscoQueueTemplate	CiscoSubdeployment
BEEERequisitionsQueue	CiscoQueueTemplate	CiscoSubdeployment
BEEEAuthorizationsQueue	CiscoQueueTemplate	CiscoSubdeployment
BEEEinboundQueue	CiscoQueueTemplate	CiscoSubdeployment

- Step 11** If your WebLogic was installed in **PRODUCTION** mode, click **Activate Changes**. Otherwise, you can skip this step.
-

## Configuring JDBC Data Sources

In this section, you will configure a JDBC Data Source to point to the ServiceCatalog database that you created in the [Configuring the Service Catalog Database](#).

Use the worksheet that you filled out at the end of the [Configuring the Service Catalog Database](#) to retrieve the necessary database information.

- 
- Step 1** Log on to the WebLogic Administration Console.
- Step 2** If your WebLogic was installed in PRODUCTION mode, click **Lock & Edit**. Otherwise, you can skip this step.
- Step 3** Choose **Services > Data Sources**.
- Step 4** Choose **New > Generic Data Source**.
- Update the information for this panel as provided in [Table 5-2](#) and click **Next**.

**Table 5-2**

Field	Value
Name	REQUESTCENTERDS
JNDI Name field	eis/REQUESTCENTERDS
Database Type drop-down list	<ul style="list-style-type: none"> <li>(For SQL Server), choose <b>MS SQL Server</b></li> <li>(For Oracle), choose <b>Oracle</b></li> </ul>

- Step 5** On the next panel, select one of the following values from the Database Driver drop-down list, then click **Next**:
- Select "Microsoft's MS SQL Server Driver (Type 4) Version:2005 and later" if your database is MS SQL Server.
  - Select "Oracle's Driver (Thin) for Instance connections; Version:9.0.1 and later" if your database is Oracle, using SID to connect.
  - Select "Oracle's Driver (Thin) for Service connections; Version:9.0.1 and later" if your database is Oracle, using Service Name to connect.
- Step 6** On the next panel, select the "Support Global Transactions" option and the "One-Phase Commit" option, then click **Next**.
- Step 7** Update the information for this panel as provided in [Table 5-3](#) and click **Next**.

**Table 5-3**

Field	Definition
Database Name	<ul style="list-style-type: none"> <li>(For SQL Server), enter the name of the database, for example, "ServiceCatalog".</li> <li>(For Oracle), enter the SID if you are using SID to connect to your Oracle database, or the Service Name if you are using Service Name to connect to your Oracle database.</li> </ul>
Host Name	Enter the database server name or IP address
Port	Enter the database port number



Table 5-3

Field	Definition
Database User Name	Enter the name of the db_owner (or schema user) of the ServiceCatalog database (for example, enter CPSCUser).
Password	Enter the password for the Database User Name
Confirm Password	Re-enter the password for the Database User Name

**Step 8** Update the information for this panel as provided in Table 5-4 and click **Next**.

**Caution**

Do not click the Test Configuration button.

Table 5-4

Field	Definition
Driver Class Name	Enter the value (one string) For SQL Server: "com.microsoft.sqlserver.jdbc.SQLServerDriver" For Oracle: "oracle.jdbc.OracleDriver"
URL	Enter the following value (one string): <b>For SQL Server:</b> jdbc:sqlserver://<db_server>:<db_port>;databaseName=<db_name> (For example, jdbc:sqlserver://mysqlserver.cisco.com:1433;databaseName=ServiceCa talog) <b>For Oracle SID:</b> jdbc:oracle:thin:@<db_server>:<db_port>:<SID> (For example, jdbc:oracle:thin:@myoracle.cisco.com:1521:PROD) <b>For Oracle Service Name:</b> jdbc:oracle:thin:@//<db_server>:<db_port>/<service_name> (For example, jdbc:oracle:thin:@//myoracle.cisco.com:1521/PRODSN)
Database User Name	Enter the name of the db_owner (or schema user) of the ServiceCatalog database (for example, enter CPSCUser).
Password	Enter the password for the Database User Name.
Confirm Password	Re-enter the password for the Database User Name.

Table 5-4

Field	Definition
Properties	<p>For SQL Server, enter the following lines:</p> <pre>userName=&lt;Database User Name&gt; selectMethod=direct</pre> <p>For Oracle, enter the following line:</p> <pre>user=&lt;Database User Name&gt;</pre>
Test Table Name	<p>For SQL Server, enter the following value:</p> <pre>SQL SELECT 1</pre> <p>For Oracle, enter the following value:</p> <pre>SQL SELECT 1 FROM DUAL</pre>

**Step 9** Choose your WebLogic Server as the Target.



**Note** If you have a WebLogic Cluster environment, then choose both the Cluster name and the “**Service Link WebLogic Server**” as the Targets for this data source.

**Step 10** Click **Finish**.

The newly created data source named “REQUESTCENTERDS” should appear on the Summary of JDBC Data Sources panel. Verify that the JNDI Name and Target information for this data source is correct.

**Step 11** Click REQUESTCENTERDS to open its properties.

**Step 12** Choose **Configuration > Connection Pool**.

**Step 13** Change the values for the following parameters on the screen:

- **Initial Capacity = 80**
- Maximum Capacity = 100
- Minimum Capacity = 80

**Step 14** Click **Save**.

**Step 15** In Connection Pool tab, at the bottom of the panel, choose **Advanced**.

**Figure 5-5 Connection Pool – Advanced Settings**

Test Connections On Reserve

Test Frequency:

Test Table Name:

Seconds to Trust an Idle Pool Connection:

361941

**Step 16** Click the **Test Connections On Reserve** option.

**Step 17** In the Test Table Name field, enter the following value, then click **Save**:

**For SQL Server:**

**SQL SELECT 1**

**For Oracle:**

**SQL SELECT 1 FROM DUAL**

**Step 18** If your WebLogic was installed in PRODUCTION mode, click **Activate Changes**. Otherwise, you can skip this step.

## Configuring Basic Authentication for NSAPIs

You would need to replace the below security configuration in config.xml for enabling basic authentication on nsAPIs. Before you start any servers in weblogic and perform deployments, add the configurations manually in the path:

C:\WL\_HOME\user\_projects\domains\mydomain\config\config.xml.

```
<security-configuration>
  <enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-credentials>
</security-configuration>
```

For cluster, add the same configuration on all the nodes.

## Restarting WebLogic Server

You must restart your WebLogic Server in order for it to pick up the new JMS Data Sources and basic authentication configurations.

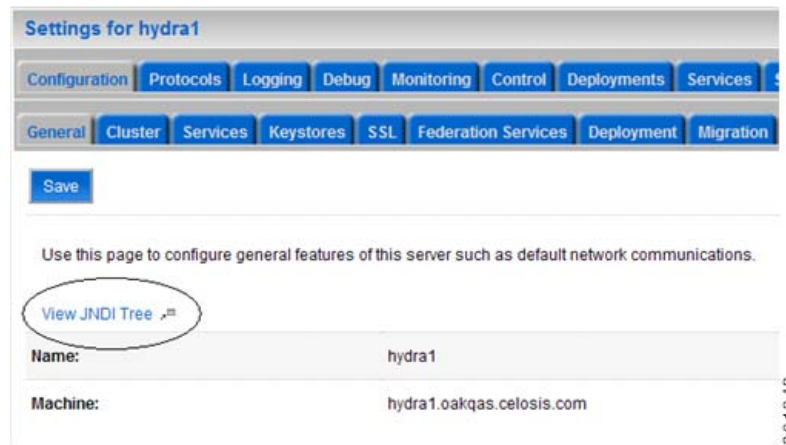
**Step 1** Restart your WebLogic Server.

**Note**

If you have WebLogic Cluster environment, restart all the WebLogic servers in the Cluster as well as the “Service Link WebLogic Server”.

**Step 2** Once the WebLogic Server is started successfully, navigate to its **Configuration > General** tab.

**Figure 5-6 JNDI Tree**



**Step 3** Click the link called **View JNDI Tree** right above the Name field. The JNDI Viewer window appears.

**Step 4** In the JNDI Tree Structure on the left hand side, look for the following entries:

```
eis> REQUESTCENTERDS
BEEEEAuthorizationsQueue
BEEEEInboundQueue
BEEERequisitionsQueue
ISEEInboundQueue
ISEEOutboundQueue
NSConnectionFactory
```

**Step 5** If you have a clustered WebLogic environment, then the JNDI Tree for your WebLogic Cluster should contain only the following entry:

```
eis> REQUESTCENTERDS
```

And the JNDI Tree for the “Service Link WebLogic Server” should contain the following entries:

```
eis> REQUESTCENTERDS
BEEEEAuthorizationsQueue
BEEEEInboundQueue
BEEERequisitionsQueue
ISEEInboundQueue
ISEEOutboundQueue
```

NSConnectionFactory

---

Complete the [WebLogic Application Server Information Worksheet](#), by entering your configuration values in the **Value** column. The information in that worksheet will be needed when you run the Prime Service Catalog Installation Wizard.

## Installing Prime Service Catalog on WebLogic Application Server

Prime Service Catalog provides two types of WebLogic installation —Typical and Custom. The Typical installation performs a streamlined installation using default settings. It requires a smaller footprint as the three foundational application components—Service Catalog application, Service Link application, and JMS service—are hosted on the same application server. Typical installation is commonly used when setting up a sandbox environment. The Custom installation allows you to configure a different deployment topology and to apply custom changes to the application. Use the Custom Installation mode if you have any of the following requirements:

- Have Service Catalog application, Service Link application, JMS service running on separate application servers
- Have a clustered Service Catalog topology (for WebLogic)
- Have separate tablespaces for definitional data, transactional data and indexes (for Oracle Only)
- Add custom content to the RequestCenter.war
- Recreate the RequestCenter.war or ISEE.war files without executing any database scripts

After your WebLogic environment is prepared, you can proceed to perform Typical or Custom installations for WebLogic.

After you finish executing the Prime Service Catalog installer successfully, follow the instructions in the next section [Postinstallation Configuration for WebLogic](#) to complete the rest of the configuration steps.

### Performing a Typical Installation

In this scenario, a new database schema is created for a new Prime Service Catalog installation. A “Typical” installation type is chosen in the installation wizard when you want to perform a streamlined installation using default settings.

#### Before You Begin

- Extract the electronic software distribution file that you downloaded from the Cisco web site to your computer, if you have not already done so.
- Add the `%JAVA_HOME%\bin` (or `$JAVA_HOME/bin` if you are on Linux) to the beginning of the `PATH` environment variable on your machine, where `%JAVA_HOME%` points to the correct JDK directory.

## Procedure

- 
- Step 1** On Windows Operating System, log in as a user with administrator rights, and double-click setup.cmd to launch the GUI installation wizard.
- On Linux Operating System, log in as the "root" user, and execute ./setup.sh from a graphical interface, such as X-window, to launch the GUI installation wizard.
- Step 2** When the Introduction panel appears, click **Next** to begin.
- Step 3** In the **Choose Install Folder** panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click **Next**.
- On Windows, the default value for destination folder is **C:\CiscoPrimeServiceCatalog**.
  - On Linux, the default value is **/opt/CiscoPrimeServiceCatalog**. The value for destination directory must not contain any space character.




---

**Note** Do not enter the installation folder of your WebLogic root directory. We recommend that you create the destination folder outside of your application server directory.

---

Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`.

For WebLogic, this directory is where the Service Catalog installer creates the WAR files for the Service Catalog application.

- Step 4** On the Application Server Selection panel, select the application server as WebLogic and click **Next**. Refer to the Application Server Information Worksheet that you filled out in Appendix A.
- Step 5** On the Installation Type panel, select **Typical** radio button and click **Next**.
- Step 6** On the Database Selection panel, select a database platform (Microsoft SQL Server or Oracle) and click **Next**. The subsequent panels may look different depending on which database platform you select at this point. Refer to the [Database Information Worksheet](#) that you filled out in Appendix A to determine your database platform.
- Step 7** On the Service Catalog Database Creation panel:
- If you have not created the database in advance, select **Yes**. By selecting **Yes**, you are telling the installer to create the database automatically for you. In the next panel, you will be prompted for the information that the installer will use to create the database user and database schema for Service Catalog. Refer to the [Database Information Worksheet](#) for the description of each field on this panel.
  - If you have already created your database, then select **No**. In the next panel, you will be prompted for the information of the existing database user and database schema. Refer to the [Database Information Worksheet](#) for the description of each field on this panel. (If you are performing an upgrade installation, you must select No. Refer to Chapter 7: [Upgrading Prime Service Catalog](#) for more detailed information).
- Step 8** On the Service Catalog Database panel, enter the information for the Service Catalog database.
- If you selected Yes in the last panel, you will see a "**Create Database**" button on this panel, and the Next button is grayed out. Notice that you need to enter the password for either the "sys" user (for Oracle) or the "sa" user (for SQL Server) which the installer will use to connect to your database server. Once you fill out the information on this panel, click the "**Create Database**" button. If you get the message "Service Catalog database created successfully", click **OK** to close the message. The **Next** button is now enabled.
  - If you selected **No** in the last panel, you just need to fill out the information for the existing Service Catalog database, and select the "Execute database scripts" check box.

**Note**

The "Create Database" feature creates a very basic Service Catalog database that meets the minimum requirements for the Service Catalog application to operate. This feature is recommended for a Demo or Test system. For a Production system, contact your DBA in advance, to create the Service Catalog database which meets all of the product requirements as described in the Configuring Databases section, as well as any performance, reliability, and security requirements that adhere to your corporate policy.

- Step 9** Click **Next** to continue. The installer connects to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if any database setting is missing. See the [Software Requirements](#) for the database requirements. If a database validation error occurs, you can do the following:
- Close the error dialog and click **Cancel** to exit the installation wizard, or
  - Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next panel.
- Step 10** In the Master Key Password panel, enter the master key password.
- As part of the security requirement, a master key password must be provided that would be used to encrypt all the passwords that are available in the application. The password provided must match the password rules, as described on the panel.
- The master key password is saved in two files, kek\_new.txt and kek\_old.txt, under the <ServiceCatalog\_Install\_Dir>/dist directory. The kek\_new.txt and kek\_old.txt files must be backed up and stored in a safe location. The application server cannot login to the ServiceCatalog database without the master key password files. If you lose these master key password files, please contact Cisco TAC for help.
- Step 11** In the Service Catalog Configuration panel, enter the information for the WebLogic server where Service Catalog application (i.e. RequestCenter.war) will be deployed. Refer to the [WebLogic Application Server Information Worksheet](#) that you have filled out in Appendix A. For more information, see [Service Catalog Configuration for WebLogic](#).
- Step 12** Click **Next** to display the Messaging Configuration panel. Enter the information for the JMS Queue Connection Factory. Refer to the [WebLogic Application Server Information Worksheet](#) that you filled out in Appendix A. For more information, see [Messaging Configuration Table](#).
- Step 13** Click **Next** to display the Messaging Queues Configuration panel. Enter the queue names as how you prepared them for your WebLogic server. Refer to the [WebLogic Application Server Information Worksheet](#) that you filled out in Appendix A.
- Step 14** Click **Next** to display the Service Catalog Administration Configuration panel. Enter details as provided in [Service Catalog Administration Configuration Table](#), and click **Next**.
- Step 15** Click **Install** in the Pre-Installation Summary panel to begin installation.
- The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.
- Step 16** If the installation process completes successfully, the **Install Complete** panel appears. Click **Done** to exit the installation wizard.

You have completed the execution of the Service Catalog installer. You can now go back to the Post installation Configuration section for the appropriate application server to complete the rest of the configuration steps.

## Performing a Custom Installation

In this scenario, a “Custom” installation type is chosen in the installation wizard to customize aspects of the installation rather than accepting the defaults.

### Before You Begin

- If you are on a Windows Operating System, stop the IIS web server.
- Extract the electronic software distribution file that you downloaded from the Cisco web site to your computer, if you have not already done so.
- Add the `%JAVA_HOME%\bin` (or `$JAVA_HOME/bin` if you are on Linux) to the beginning of the `PATH` environment variable on your machine, where `%JAVA_HOME%` points to the correct JDK directory.

### Procedure

- 
- Step 1** On Windows Operating System, log in as a user with administrator rights, and double-click **setup.cmd** to launch the GUI installation wizard.
- On Linux Operating System, log in as the "root" user, and execute **./setup.sh** from a graphical interface, such as X-window, to launch the GUI installation wizard.
- Step 2** When the Introduction panel appears, click **Next** to begin.
- Step 3** In the Choose Install Folder panel, enter a directory path (or click the Choose button to select a directory) as the destination folder for Service Catalog, and click Next.
- On Windows, the default value for destination folder is **C:\CiscoPrimeServiceCatalog**
  - On Linux, the default value is **/opt/CiscoPrimeServiceCatalog**. The value for destination directory must not contain any space character.




---

**Note** Do not enter the installation folder of your WebLogic root directory. We recommend that you create the destination folder outside of your application server directory.

---

Throughout this document, this destination folder is referred to as `<ServiceCatalog_Install_Dir>`. For WebLogic, this directory is where the Service Catalog installer creates the generated WAR files for the Service Catalog application. For WildFly, this directory is also where the Service Catalog installer installs and configures the WildFly Application Server software.

- Step 4** On the Application Server Selection panel, select one of the Application server radio buttons and click **Next**.
- Step 5** On the Installation Type panel, select **Custom** radio button and click **Next**.
- Step 6** Select a component in the Component Selection panel and click **Next**.
- The Custom installation mode for WildFly allows you to install



- only the Service Catalog server,
- only the Service Link server, or
- both Service Catalog and Service Link servers on the same computer.

**Step 7** Choose the database platform (Microsoft SQL Server or Oracle) you want, on the Database Selection panel and click **Next**.

The subsequent panels may look different depending on the database platform you select. Refer to the [Database Information Worksheet](#) to determine your database platform.

**Step 8** On the Service Catalog Database Creation panel:

- If you have not created the database in advance, select Yes. By selecting Yes, you are telling the installer to create the database automatically for you. In the next panel, you will be prompted for the information that the installer will use to create the database user and database schema for Service Catalog. Refer to the [Database Information Worksheet](#) for the description of each field on this pane.
- If you have already created your database, then select No. In the next panel, you will be prompted for the information of the existing database user and database schema. Refer to the [Database Information Worksheet](#) for the description of each field on this panel. (If you are performing an upgrade installation, you must select No. Refer to [Chapter 6, "Upgrading Prime Service Catalog"](#) for more detailed information.)

**Step 9** On the Service Catalog Database panel, enter the information for the ServiceCatalog database.

- If you selected Yes in the last panel, you will see a "**Create Database**" button on this panel, and the Next button is grayed out. Notice that you need to enter the password for either the "sys" user (for Oracle) or the "sa" user (for SQL Server) which the installer will use to connect to your database server. Once you fill out the information on this panel, click the "**Create Database**" button. If you get the message "ServiceCatalog database created successfully", click **OK** to close the message. The **Next** button is now enabled.
- If you selected **No** in the last panel, you just need to fill out the information for the existing ServiceCatalog database, and select the "**Execute database scripts**" check box.



**Note** The "Create Database" feature will create a very basic ServiceCatalog database that meets the minimum requirements for the Service Catalog application to operate. This feature is recommended for a Demo or Test system, but for a Production system, it is advisable that you work with your DBA to create the ServiceCatalog database in advance which meets all of the product requirements as described in the [Configuring Databases](#) section, as well as any performance, reliability, and security requirements that adhere to your corporate policy.

**Step 10** Click **Next**.

The installer will connect to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if it detects that certain required database setting is missing. (Refer to [Configuring the Service Catalog Database](#) for the database requirements.) If a database validation error occurs, you can do the following:

- Close the error dialog and click **Cancel** to exit the installation wizard, or
- Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next panel.

**Step 11** On the Master Key Password panel, enter the master key password.

The password provided must match the password rules, as described on the panel. The master key password is saved in two files, `kek_new.txt` and `kek_old.txt`, under the `<ServiceCatalog_Install_Dir>/dist` directory.

The `kek_new.txt` and `kek_old.txt` files must be backed up and stored in a safe location. The application server cannot login to the Service Catalog database without the master key password files. If you lose these master key password files, please contact Cisco TAC for help.

**Step 12** On the Service Catalog Configuration panel:

- Enter the information for the WebLogic server where Service Catalog application (i.e. `RequestCenter.war`) will be deployed. Refer to the [WebLogic Application Server Information Worksheet](#) that you have filled out in Appendix A. For more information, see [Service Catalog Configuration for WebLogic](#).
- Click the **Advanced Options**. For WebLogic, select the Enable Clustering option if you have a Clustered WebLogic environment. For information on other advanced options details see, [Advanced Options Table for Service Catalog Configuration panel](#).
- Click **Close** in the Advanced Options window and Click **Next**.

The Service Link Configuration window is displayed.

**Step 13** Enter the information for the WebLogic server where Service Link application (i.e. `ISEE.war`) will be deployed and Click **Next**. Refer to the Application Server Information Worksheet that you have filled out earlier. See [Service Link Configuration Table for Custom Installation using WildFly Server](#).



**Note**

If Service Catalog is deployed in a Clustered WebLogic, then Service Link must be deployed in a separate WebLogic server that does not belong to the Cluster.

**Step 14** In the Messaging Configuration window enter information for the JMS Queue Server and Click **Next**. Refer to the [WebLogic Application Server Information Worksheet](#) that you filled out in Appendix A. For more information, see [Messaging Configuration Table for Custom Installation](#).

**Step 15** Click **Next** to display the Messaging Queues Configuration panel. Enter the queue names as how you prepared them for your WebLogic server. Refer to the [WebLogic Application Server Information Worksheet](#) that you filled out in Appendix A.

**Step 16** On the Service Catalog Administration Configuration panel, enter the information for the SMTP server, and the password for the Site Administrator. Refer to the [Service Catalog Administration Configuration Table](#) for the description of each field on this panel. Click **Next**.

**Step 17** Click **Install** in the Pre-Installation Summary panel to begin installation.

The installer will display the progress bar. It may take up to 30 minutes for the installer to complete. Do not interrupt or abort the installer during this process.

**Step 18** If the installation process completes successfully, the **Install Complete** window appears. Click **Done** to exit the installation wizard.

You have completed the execution of the Service Catalog installer. You can now go to the [Postinstallation Configuration for WebLogic](#) section to complete the rest of the configuration steps.

# Postinstallation Configuration for WebLogic

When the Prime Service Catalog installation wizard completes, it creates the following WAR files underneath the “<ServiceCatalog\_Install\_Dir>\dist” directory:

- RequestCenter.war
- ISEE.war

The Prime Service Catalog installation wizard did not automatically deploy these WAR files on your WebLogic Server. You need to follow the instructions in this section to manually deploy these WAR files. See the WebLogic Application Server Information Worksheet that you filled out in Appendix A to get the parameter values needed during the deployment.

## Extracting WAR Files

You must deploy **RequestCenter.war** and **ISEE.war** in extracted format. To extract the WAR files:

- 
- Step 1** Create a subdirectory called **applications** underneath the “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>” directory, if it does not already exist. Note that you perform this task on the computer where the WebLogic Administration Server is running.
- Step 2** Create three subdirectories underneath “applications” as follows:
- WL-Management
  - ServiceLink
  - RequestCenter
- Step 3** Extract the WAR files (generated by the Prime Service Catalog installation wizard) into the new directories that you just created:
- Unzip file “<ServiceCatalog\_Install\_Dir>\dist\ISEE.war” into the “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications\ServiceLink” directory.
  - Unzip file “<ServiceCatalog\_Install\_Dir>\dist\RequestCenter.war” into the “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications\RequestCenter” directory.

**Note**

After extracting all the war files, ensure that you delete the .war files from original path.

**Note**

If the RequestCenter or ServiceLink subdirectory under the “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications” directory is not empty, you must first empty the entire directory before extracting the contents of the new RequestCenter.war or ISEE.war file into it. This is because the unzip utility may only overwrite files with the same names. There may be some “remnants” of old files in your destination directory that may be inadvertently deployed.

## Deploying the WAR Files to Managed Server

The war files must be deployed only in the following sequence:

- wls-management-services.war see section [Extracting and Deploying wls-management-services.war, page 5-24](#)
- ISEE.war, see section [Deploying ISEE.war, page 5-24](#)
- RequestCenter.war, see section [Deploying RequestCenter.war, page 5-25](#)

### Extracting and Deploying wls-management-services.war

Perform the following steps to extract deploy wls-management-services.war file:

- 
- Step 1** Log on to the WebLogic Administration Console.
  - Step 2** Stop all the server instances standalone or cluster and then stop the weblogic server, nodemanagers etc.
  - Step 3** Move the wls-management-services.war from /WL\_HOME/server/lib of node1 cluster/standalone to the path “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications\WL-Management”.
  - Step 4** Delete the wls-management-services.war from /WL\_HOME/server/lib of node 2.
  - Step 5** Delete the /tmp folder from AdminServer, and from and Service Link server node 1 and Request Center server on node 1 and node 2.
  - Step 6** In case you are redeploying the WL-Management, delete the war files from the /mydomain/config/deployment folder. You may skip this step for fresh installation.
  - Step 7** Ensure that wls-management-services.war exists only in the “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications folder.
  - Step 8** Start the node-managers on node 1 and node 2, and the weblogic server on node1.
  - Step 9** Start the server instance for the Service Link.
  - Step 10** Start the server instance for the RequestCenter. In a cluster, start both the server-instances (node1 and node2).
  - Step 11** Deploy the wls-management-services.war to the cluster or RequestCenter Server instance in case of standalone and bring it to STATE\_ACTIVE.
  - Step 12** Click on the deployed wls-management-services.war that is deployed and is in STATE\_ACTIVE state and change the deployment order to 1. Activate the change.
  - Step 13** Deploy the Service Link to the server instance meant for service link and bring it to STATE\_ACTIVE.
  - Step 14** Deploy the RequestCenter to the serve instance meant for the RequestCenter. If a cluster, deploy the RequestCenter to cluster. Bring it to STATE\_ACTIVE.
- 

### Deploying ISEE.war

Perform the following steps to deploy ISEE.war file:

- 
- Step 1** Log on to the WebLogic Administration Console.

- Step 2** Start your WebLogic Server if it is not already running (if you have a WebLogic Cluster environment, then start the “Service Link WebLogic Server”. The Service Link application cannot be deployed on a Cluster).
- Step 3** If your WebLogic was installed in PRODUCTION mode, click **Lock & Edit** so that you can proceed to make changes. Otherwise, you can skip this step.
- Step 4** In the left pane, click **Deployments**.
- Step 5** Click **Install**.
- Step 6** Browse to (or enter the full pathname of) the directory “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications.” You should see the two subdirectories called “RequestCenter” and “ServiceLink”.
- Step 7** Click the radio button for **ServiceLink**, then click **Next**.
- Step 8** Choose the **Install this deployment as an application** option, then click **Next**.
- Step 9** Choose your WebLogic Server as the Target. (If you have a WebLogic Cluster, choose the stand-alone “Service Link WebLogic Server” as the Target.) Then click **Next**.
- Step 10** Enter **ServiceLink** in the **Name** field. Select the **Copy this application onto every target for me** option. Click **Next**.
- Step 11** Choose the **No, I will review the configuration later** option, then click **Finish**. The progress indicator begins. This may take several minutes to complete.
- Step 12** Wait until the screen is refreshed to show that the “ServiceLink” application has State=Active and Health=OK. If your WebLogic Application Server was installed in PRODUCTION mode, then the State may be set to “Prepared” until you click **Activate Changes**.
- 

## Deploying RequestCenter.war

Perform the following steps to deploy RequestCenter.war file:

---

- Step 1** Log on to the WebLogic Administration Console.
- Step 2** Start your WebLogic Server (or WebLogic Cluster) if it is not already running.
- Step 3** If WebLogic was installed in PRODUCTION mode, click **Lock & Edit** so that you can proceed to make changes. Otherwise, you can skip this step.
- Step 4** In the left pane, click **Deployments**.
- Step 5** Click **Install**.
- Step 6** Browse to (or enter the full pathname of) the directory “<ORACLE\_HOME>\user\_projects\domain\<your\_domain>\applications.” You should see the two subdirectories called “RequestCenter” and “ServiceLink”.
- Step 7** Click the radio button for **RequestCenter**, then click **Next**.
- Step 8** Choose the **Install this deployment as an application** option, then click **Next**.
- Step 9** Choose your WebLogic Server (or WebLogic Cluster) as the Target, then click **Next**.
- Step 10** Enter **RequestCenter** in the **Name** field. Select the **Copy this application onto every target for me** option. Click **Next**.
- Step 11** Choose the **No, I will review the configuration later** option, then click **Finish**. The progress indicator begins. This may take several minutes to complete.

- Step 12** Wait until the screen is refreshed to show that the “RequestCenter” application has State=Active and Health=OK. If your WebLogic Application Server was installed in PRODUCTION mode, then the State may be set to “Prepared” until you click **Activate Changes**.
- 

## Verifying Your Installation

Perform the following steps to verify your installation:

- 
- Step 1** Test your installation by opening a new browser window and connect to the following URL:  
`http://<AppServer_Host>:<Port>/RequestCenter`  
 where <AppServer\_Host> = the host name of your WebLogic Server, and <Port> = the port number used by your WebLogic Server.  
 For example,  
`http://myps.c.mydomain.com:8001/RequestCenter`
- Step 2** Log in as the Site Administrator. For a new installation of Service Catalog, the username for the Site Administrator is "admin" and the password is the value you entered on the Service Catalog Administration Configuration panel of the installation wizard.
- Step 3** Navigate to the Service Link Module.
- Step 4** On the left hand side of the panel, under Service Link Status, verify that the connection has a green status.  
 You have completed the installation for Cisco Prime Service Catalog on WebLogic.
- 

## Redeploying a Server

In order to apply patch, perform an upgrade, or any maintenance activity which requires starting and stopping WebLogic services may require you to redeploy a server. Perform the following steps to redeploy a server:

- 
- Step 1** Log on to the WebLogic Administration Console.
- Step 2** Ensure that the RequestCenter, ServiceLink, and WL-Management deployment is in preparation state. Select the respective deployments and click **Stop**.
- Step 3** Stop the managed server created to deploy Service Link (Standalone).
- Step 4** Stop the managed server(s) created to deploy Request Center and WL-Management (cluster or standalone).
- Step 5** Start the managed server created to deploy Service Link and make sure it is up.
- Step 6** Start the managed server(s) created to deploy RequestCenter and WL-Management.  
 Once all the managed servers are up, all the deployments will have *Prepare* status.
- Step 7** Navigate back to deployment and start WL - management, Service Link, and Request Center.

**Step 8** Ensure that all the servers are in *Active* state.

---

## Configuring Web Server

At this time, you should configure the plugin for your Web Server to point to your WebLogic Server (or your WebLogic Cluster). The following Web Servers are supported with WebLogic Server:

- Red Hat Http Server 2.4.6
- IIS 8.5

This chapter does not contain instructions on how to configure your Web Server Plugin. Any plugin configurations between your Web Server and WebLogic are not handled by the Prime Service Catalog installer program. There is no Cisco library or binary that needs to be installed or configured on your Web Server installation. You should follow instructions provided by either Oracle (for WebLogic Plugin) or by the vendor of your web server.

This section contains only examples of the settings that you may want to add to your web server configuration file.

The following are examples for the settings for **Http Web Server** in standalone mode. Add the following entries to the end of file **httpd.conf**:

```
LoadModule weblogic_module modules/mod_wl_24.so

<IfModule mod_weblogic.c>
WebLogicHost m1.mydomain.com
WebLogicPort 8001
</IfModule>

<Location /RequestCenter>
SetHandler weblogic-handler
PathTrim /
</Location>
```

The following is the example for the settings for **Http Web Server** in Cluster mode.

```
LoadModule weblogic_module modules/mod_wl_24.so

<IfModule mod_weblogic.c>
    WebLogicCluster <weblogic>:8001, <weblogic>:8002
</IfModule>

<Location /RequestCenter>
SetHandler weblogic-handler
PathTrim /
</Location>
```

The following are examples for the settings for **IIS 8.5 Web Server**. Add the following entries to file **iisproxy.ini**:

```
WebLogicHost=m1.mydomain.com
WebLogicPort=8001
ConnectTimeoutSecs=20
ConnectRetrySecs=5
KeepAliveEnabled=true
KeepAliveSecs=20
WlForwardPath=/RequestCenter
```

After you complete the Plugin configuration, you need to restart both the Web Server and the WebLogic Application Server.

Repeat the steps described in the [Verifying Your Installation](#) to verify that your Web Server plugin is configured correctly to point to your WebLogic Server. However, this time connect to the following URL

`http://<WebServer_Host>:<WebServer_Port>/RequestCenter`

where `<WebServer_Host>` = the host name of your Web Server, and `<WebServer_Port>` = the port number used by your Web Server (omit the port number if it is set to 80).

For example,

`http://mywebserver.mydomain.com/RequestCenter`





# Upgrading Prime Service Catalog

## Overview

This chapter describes how to perform an upgrade from a previous release of Cisco Prime Service Catalog to this release.

## Release Upgrade Path

This upgrade process supports direct database component upgrade from Service Catalog Release 10.1 or above to Release 12.1. To bring the database schema to the supported upgrade level, the database installer program for the most recently available service pack, as listed in [Table 6-1](#) below, has to be executed against the database.

**Table 6-1**      *Direct Upgrade Paths*

From Release Version	To Release Version
11.0	12.1
11.1	12.1
11.1.1	12.1
12.0	12.1
12.0.1	12.1

If you are upgrading from releases prior to 11.0, first upgrade your installation to release 11.0 using the 11.0 installer. Then without starting the Prime Service Catalog instance, run the 12.1 installer to upgrade the instance to release 12.1.

## Limitations and Notes

The following section includes product limitation or important notes that should be considered when upgrading to this version.

### New Platform Support

Please refer to the [Cisco Prime Service Catalog Compatibility Matrix](#) for changes in platform support in this release.

Highlights of the new platforms are:

- For release to release upgrade, use a new folder as installation directory, instead of using the existing directory. However, you can continue using an existing database.
- Make sure KEK\_new.txt file is saved. And while upgrading you will be prompted to provide kek\_new.txt, the file that you saved from previous installation should be provided to continue the installation. If KEK doesn't match you will not be able to start the Prime Service Catalog.
- Operating System: Prime Service Catalog will only support Windows Server 2012 R2 and Red Hat Enterprise Linux Server 7.3. If your existing Prime Service Catalog installation was done on a different Windows or Linux Operating System, make sure that you set up new machines with the newly supported Operating System, and prepare the machines with all the necessary prerequisites.
- SQL Server: If your existing database is on SQL Server 2008, you must perform the tasks described in the [Preparing the Upgrade Environment](#) section, prior to running the upgrade for Prime Service Catalog.
- Oracle: If your existing database is on Oracle 12c, you must perform the tasks described in the [Preparing the Upgrade Environment](#) section, prior to running the upgrade for Prime Service Catalog.
- Audit Log Data: Before the upgrade, migrate the Audit Log data from previous release Prime Service Catalog 10.1/11.0/12.0 to Prime Service Catalog 12.1. For more information, see [Migrating the Audit Log Data](#) section.

After the upgrade is completed, disable the Change Data Capture feature as detailed in [Step 8](#) of the [Performing Post-upgrade Tasks](#).

- WebSphere: WebSphere Application Server is no longer supported. Please contact Cisco TAC if you have WebSphere, and is interested in upgrading to Prime Service Catalog 12.1.
- Oracle Java: Oracle JDK 8 Update 91 (or higher update) must be used for WildFly on Windows Operating System, and for WebLogic Application Server on any Operating System. You must install Oracle JDK 8 Update 91 (or higher update) on your machine prior to running the upgrade for Prime Service Catalog. For WebLogic, modify the JAVA\_HOME property in your WebLogic's commEnv.cmd (or commEnv.sh) script to use the correct version of JDK. If you have a clustered WebLogic environment, you must perform this step on every node in the cluster.
- OpenJDK: Red Hat OpenJDK 8 (version 1.8.0\_91 or higher 1.8.0\_x) must be used for WildFly on Red Hat Enterprise Linux Operating System. You must install OpenJDK 1.8.0\_91 (or higher 1.8.0\_x) on your machine prior to installing Prime Service Catalog.
- WebLogic: Ever since release 10.0 of Prime Service Catalog, WebLogic 12c (12.2.1) must be used. If you are on an older release of Prime Service Catalog and use an older version of WebLogic, you must first upgrade your WebLogic to version 10.3.6 or install a brand new WebLogic 12c (12.2.1) environment, and configure your WebLogic server as described in Chapter 5, prior to running the upgrade for Prime Service Catalog.
- Browser: Please refer to the Cisco Prime Service Catalog Compatibility Matrix for a list of new browsers that are supported for this release of Prime Service Catalog.

## Rating Facet

If you have an existing facet with display name as **Rating**, make sure that you rename this facet before upgrading. This is to avoid conflict with the new Rating facet available in current Cisco Prime Service Catalog release.

## New JDBC Drivers

New JDBC drivers for Oracle and SQL Server are shipped with this release of Prime Service Catalog. If you are using WebLogic application server, you will need to delete the existing REQUESTCENTERDS datasource (which used the DataDirect driver in newScale\_drivers.jar), and recreate the REQUESTCENTERDS datasource using the new JDBC driver (either ojdbc7.jar for Oracle or sqljdbc4.jar for SQL Server). More details are described in the [Preparing the Upgrade Environment](#) section.

**Note**

If you have any customization that makes use of the newScale unified driver, it has to be replaced with the appropriate JDBC driver based on the database type.

## Service Import/Export Not Backwards Compatible

Service Import/Export is not backwards compatible to previous releases. Services exported in prior releases cannot be imported to this release. Please be sure to export any services you maintain in a code repository after the upgrade is complete.

## Catalog Deployer Packages Not Backwards Compatible

Due to the change in the XML format in Catalog Deployer, packages in “Deployed” or “Received for Deployment” status are no longer usable. The content also may not render. For this reason, all packages pending deployment should be processed before upgrading to Release 12.1.

## What is Upgraded

The upgrade process outlined in this chapter upgrades Service Catalog software as well as the Service Catalog database to support new capabilities provided in Service Catalog. These capabilities include more stringent control over data and referential integrity, ensuring enhanced data quality of the Service Catalog database.

## What is Not Upgraded

The upgrade process identifies all objects in the existing database that are not recognized as part of the application schema.

- Unrecognized objects are automatically removed from the database, if they interact with any Service Catalog tables. For examples, the following objects (if they exist) will be dropped:
  - An unrecognized index on a Service Catalog table.
  - An unrecognized trigger on a Service Catalog table.
  - An unrecognized constraint on a Service Catalog table.
  - An unrecognized foreign key constraint that points to a Service Catalog table.
- All other types of unrecognized objects that do not interact with Service Catalog tables will only be reported and not dropped. For examples, the following objects (if they exist) are left alone: tables, columns, sequences, stored procedures, functions, and indexes that do not reference Service Catalog tables, constraints that do not affect Service Catalog tables.

## Assumptions and Best Practices

- You must create and validate database backups and file system backups before upgrading. This is critical because you can rollback an upgrade only by restoring your databases and file system manually; no rollback function is built into the upgrade program.
- The production site will be down during the upgrade process, so you should schedule the upgrade for maintenance periods.
- You are upgrading from 10.0 or later. See the [Release Upgrade Path](#).

## Prerequisites

- A sandbox environment for upgrade.
- Database backups and a well-rehearsed restore process.
- A complete list of all customizations (custom style sheets, JavaScript libraries, LDAP Java mapping code, and so on.)
- All databases should meet the requirements as stated in the [Configuring the Service Catalog Database](#).

## High-Level Upgrade Procedure

Your organization most likely has already developed an upgrade methodology for Service Catalog solutions or has best practices for other enterprise software upgrades. The methodology described in this guide is useful to either follow as an alternate or to augment your established practices for specific new upgrade requirements.

We recommend that you create a sandbox environment where you rehearse a dry run of the upgrade procedures for your existing Service Catalog system. Take notes of any technical issues and resolutions that may arise along the way. This will help you prepare for the actual upgrade of your production system. This dry run exercise will also provide you with an overall timeline of the upgrade process from beginning to end, which can help you plan the appropriate system downtime needed to complete the upgrade of your production system.

Once you can successfully upgrade the system in your sandbox environment and feel comfortable with the process, you can schedule the upgrade of your production system, and repeat the same process by following the instructions in this guide, in conjunction with the technical notes that you prepared during the dry run exercise.

At a high level, the upgrade procedures are as follows:

---

**Step 1** Back up the current production databases and restore them onto another set of databases.



**Note**

---

You must restore your database backups onto a brand new SQL Server 2012 SP3 or 2016 database or an Oracle 12c database.

---

- Step 2** Create a sandbox environment that has all the prerequisites for Release 12.1, including new version of application server, Java and JDBC driver. This is the environment where you will be executing the upgrade program from the Release 12.1 package and needs to be configured to connect to the copy of production databases.
- Step 3** Execute the Service Catalog setup program as described in the [Installing Prime Service Catalog on WildFly Application Server](#) or [Installing Prime Service Catalog on WebLogic Application Server](#). On the Service Catalog Database panel of the installation wizard, enter the connection information for the copy of the production database.
- Step 4** Click **Next**.
- Step 5** Click **Upgrade Existing Database**.
- Step 6** Click **Validate Schema**.
- Step 7** Click **View Errors**. If any schema errors in your database are reported, work with your database administrator and application programmer to fix the schema errors. Some schema errors may come with a *suggested* SQL command to fix the error, which you can discuss with your DBA and application programmer to see if it is applicable for your error condition. Others may require that you consult with the Cisco Technical Assistance Center (TAC) to come up with an appropriate fix. Document all of the validation errors and resolutions you encounter.
- Step 8** Click **Validate Schema** iteratively after each time you fix the validation errors, until there are no more errors reported.
- Step 9** Click **Validate Data**.
- Step 10** Click **View Errors**. If any data errors in your database are reported, work with your database administrator and application programmer to fix the errors in the data. There are two types of data errors—Validation Errors and Auto-Repairable Errors. Some validation errors may come with a *suggested* SQL command to fix the error, which you can discuss with your DBA and application programmer to see if it is applicable for your error condition. Others may require that you consult with the Cisco Technical Assistance Center (TAC) to come up with an appropriate fix. Document all of the validation errors you encounter and the resolutions that you come up with.
- Step 11** Click **Validate Data** iteratively after each time you fix the validation errors, until no Validation Errors are reported. It is OK to have some Auto-Repairable Errors. They will be programmatically fixed in the next step.
- Step 12** Click **Repair Database**. This function will programmatically fix all Auto-Repairable Errors reported in the previous step.
- Step 13** When the repair database function completes, click **Next** to complete the remaining pages of the Service Catalog installation wizard.
- Step 14** After the installation wizard completes the upgrade installation, reapply any necessary customizations on your sandbox environment.
- Step 15** Perform user acceptance testing for the upgraded system in the sandbox environment.
- Step 16** Gather all of the technical notes that you have created along the way.
- Step 17** At this point, if you feel that you are still not comfortable with the upgrade process, you may want to clean up your sandbox environment, and repeat all steps one more time in the sandbox environment. This time, follow the instructions in this guide, in conjunction with the technical notes that you have documented so far.
- Step 18** When you are ready, repeat the entire upgrade process on your production environment.
-

# Upgrading Prime Service Catalog

Several platforms have been de-supported since Release 12.1. Therefore, review Release Upgrade Path to find out whether you need to upgrade the versions of the database, application server, Java, web server, or Operating System, prior to upgrading Prime Service Catalog.

If the platform that your existing Service Catalog is running on is no longer supported, you need to prepare a new environment for one of the newly supported platforms, as described in [Chapter 2, “Installation Requirements”](#).

Upgrading Service Catalog involves:

- Performing preupgrade tasks while the current version of the application is up and running
- Preparing a sandbox environment that meets the newly supported platforms and prerequisites for the Service Catalog Release 12.1 installation
- Running the Service Catalog installation wizard and selecting Upgrade Existing Database.
- Validating the integrity of preupgrade database, and repairing any schema or data issues found
- Performing post-upgrade tasks

The upgrade procedures are described in more detail in the following sub-sections:

- [Performing Preupgrade Tasks, page 6-6](#)
- [Preparing the Upgrade Environment](#)
- [Run the Installation Wizard to the Validation Page](#)
- [Validating Database](#)
- [Validating Schema](#)
- [Validating Data](#)
- [Repairing the Database](#)
- [Completing Installation](#)
- [Performing Post-upgrade Tasks](#)

## Performing Preupgrade Tasks

Perform the following mandatory preupgrade tasks on your production environment.

- 
- Step 1** If you do not have the Advanced Reporting module, proceed to Step 2. Otherwise, you need to perform several preupgrade tasks for the Advanced Reporting module, as described in the [Performing Preupgrade Tasks for Reporting](#). Perform only the preupgrade steps for the Advanced Reporting module, then return to this section, and complete the rest of the procedures outlined here.
- Step 2** If there are application server version changes, the unprocessed messages residing in the JMS queues for Service Link will not be migrated automatically to the new application servers. Prior to upgrade, you should check that there are no unprocessed messages in the queues and resolve any that may be present. Once the queues are clear, stop all Service Link agents, so that you have a chance to verify Service Link communication before any agent is restarted after upgrade.
- Step 3** Catalog Deployer does not support deploying packages between different release levels of Service Catalog. Therefore, prior to upgrade, ensure that you have deployed all assembled packages that are ready for deployment. Otherwise, you will not be able to deploy them after your database is upgraded to

Release 12.1. Furthermore, as you approach the time for the upgrade, for any new package that you assemble in your current system, you might want to include the release version of Service Catalog in the description. This will make it easier for you to identify different release versions of packages.

- Step 4** An optional activity that may be included in the preupgrade checklist is to review the list of deployed packages. You may want to export and delete the packages that no longer need to be maintained online. Since these packages can no longer be deployed (once the upgrade has taken place), keeping them online is useful only for querying deployment history. By deleting these packages, you recover space in the database. Such clean-up activities can be conducted in all systems (development, test/QA, and production).
  - Step 5** Stop all Service Catalog services on the application server.
  - Step 6** Back up all Service Catalog databases. Make sure that you back up all Service Catalog-related databases if you have more than one. For example, in addition to the Service Catalog database, you may have a separate Data Mart database or Content Store database (which is used by Cognos). If so, you need to back up all databases.
  - Step 7** Back up all customization scripts or files. The upgrade process will not preserve any customizations on your existing installation. Therefore, after the upgrade, you may need to reapply some or all of these customizations on your system if they are still applicable.
  - Step 8** Back up the installation directory. Back up the directory where you originally installed the Service Catalog software.
  - Step 9** Migrate the Audit Log Data. See [Migrating the Audit Log Data](#).
  - Step 10** Proceed to the [Preparing the Upgrade Environment](#) section below.
- 

## Migrating the Audit Log Data

To migrate the Audit Log data from an older release (such as 10.1 on Oracle 11g) to the current release (12.1 on Oracle 12c), the CDCADMIN schema should be imported into the current release.

Before the upgrade process, run the following commands to create the appropriate table spaces in the current release:

### 1. create table space cdc\_tbsp

```
CREATE TABLESPACE cdc_tbsp DATAFILE
'cdctbsp.dbf' SIZE 525M AUTOEXTEND ON NEXT 512M MAXSIZE 20G
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 1m
SEGMENT SPACE MANAGEMENT AUTO;
```

### 2. create schema cdcadmin

```
CREATE USER cdcadmin
IDENTIFIED BY cdcadmin
DEFAULT TABLESPACE cdc_tbsp
TEMPORARY TABLESPACE temp
QUOTA UNLIMITED ON cdc_tbsp;
```

After executing the above commands, ensure that the RCUser schema is prepared in the same name as was used earlier, and then import the Audit Log data into the CDCADMIN schema, which was created now.

## Preparing the Upgrade Environment

Skip this section if you are ready to perform the upgrade on your production environment.

In this section, you will be creating a sandbox environment which you will use to perform the dry run exercise for the upgrade process. Once you are comfortable with the upgrade process and are armed with the technical notes that you have collected during the dry run exercise, you can then begin the upgrade procedures on the actual production system.

### Before you Begin

Perform the mandatory preupgrade tasks in [Performing Preupgrade Tasks, page 6-6](#).

To prepare a sandbox environment:

- Step 1** Restore the production database backups onto another set of databases. If you have enabled Audit Logs in Service Catalog Version 10.1 in your SQL Server environment, execute the following commands to display Audit Log records when restoring database during an upgrade from Service Catalog Version 10.1 to 12.1:

When restore is to be done on same host:

```
RESTORE DATABASE DB_101_RESTORE FROM DISK='C:\Databases\Backup\DB_101.bak'
WITH
MOVE 'DB_101' TO 'C:\Databases\Backup\DB_101.mdf',
MOVE 'DB_101_log' TO 'C:\Databases\Backup\DB_101_log.ldf'
, KEEP_CDC
```

When restore is to be done on a different host:

```
RESTORE DATABASE DB_101_RESTORE FROM DISK='C:\Databases\Backup\DB_101.bak'

WITH
MOVE 'DB_101' TO 'C:\Databases\Backup\DB_101.mdf',
MOVE 'DB_101_log' TO 'C:\Databases\Backup\DB_101_log.ldf'
, KEEP_CDC

USE DB_101_RESTORE
GO
EXEC sys.sp_cdc_add_job 'capture'
GO
EXEC sys.sp_cdc_add_job 'cleanup'
GO
```



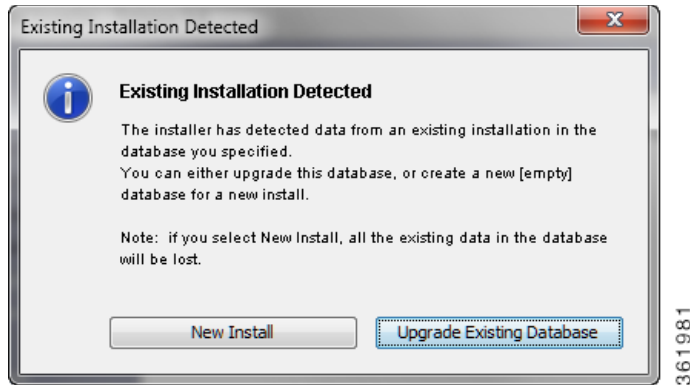
### Note

Audit Logs are displayed by default for database backup operations during a direct upgrade of Service Catalog 10.1 to Service Catalog 12.1.

- Step 2** If you are using Oracle DBMS, it is recommended that you execute recompile the statistics for each database after it is restored. This step is essential for enhancing the performance of upgrade processes on large databases. Make sure that you meet all the requirements as described in the “Configuring Oracle” section of Chapter 3.
- Step 3** If your database is SQL Server, you must activate the READ\_COMMITTED\_SNAPSHOT by performing the following:
- Connect to your SQL Server as the “sa” user, and set the SQL Server in single-user mode.





**Figure 6-1 Existing Installation Detected****Step 4** Click **Upgrade Existing Database**.

The Validation page of the installation wizard appears.

The Service Catalog installation wizard will not allow you to upgrade an existing database until it has been successfully validated and repaired. The Validation page is designed so that the functions are executed in sequential order:

1. Validate Schema
2. Validate Data
3. Repair Database

You cannot execute Validate Data without having executed Validate Schema at least once. You cannot execute Repair Database without having executed Validate Data at least once.

You can execute each function multiple times. However, each time that you execute Validate Schema, the program reinitializes as if you start the validation process from the beginning. For example, let's say you have just completed Validate Data. You can proceed with Repair Database. But, instead you choose to execute Validate Schema again. Because you execute Validate Schema, the system is reinitialized, and thus after you complete Validate Schema, you cannot jump to Repair Database. You must execute Validate Data next.

**Step 5** Proceed to the [Validating Database](#) section below.

## Validating Database

Skip this section and proceed to the [Validating Schema](#) section if you are already familiar with the database validation process during the Prime Service Catalog upgrade. You can always come back to review this section when the Validate Schema and Validate Data steps return any error.

The functions on the Validation page verify the integrity of your existing schema and database. The results for all validation scripts are stored in a table called SchValidationLog in the database. See the [SchValidationLog Table](#) for instructions to view this log file. All possible validation entry ErrorLevels and their descriptions are shown in [Table 6-2](#) below.

**Table 6-2 Validation ErrorLevels**

ErrorLevel	Description
inform	<p>The validation test results in an anomaly that is deemed harmless for the upgrade process, as well as for the application. For example, the validation detects a table that does not belong to the database schema. The existence of this table will not cause the upgrade to fail, nor will it have any ill effect on the application.</p> <p>These unrecognized objects that do not interact with Service Catalog tables are flagged with a status of “inform” in the SchValidationLog table. The following objects (if they exist) are reported only: tables, columns, sequences, stored procedures, functions, indexes and constraints that do not interact with Service Catalog tables. These objects are reported only, and are left alone.</p> <p>All validation entries with ErrorLevel= “inform” will be ignored.</p> <p>No action is required on your part to address these entries.</p>
inform: auto-repairable	<p>The data validation test results in a data error that is deemed to be harmful. However, this type of error can be safely and programmatically fixed by the Repair Database function.</p> <p>Most errors of this type are the result of internal inconsistencies, possibly introduced by previous upgrades or import utilities, and the repair typically consists of restoring referential or data integrity.</p> <p>The RepairScript column in the SchValidationLog table shows the SQL statement that is used to repair the error.</p> <p>No action is required on your part.</p>
inform: auto-repaired	<p>The Repair Database function executes the sql statement documented in the RepairScript column to fix the error that was reported as “inform: auto-repairable” above.</p> <p>All validation entries with ErrorLevel= “inform:auto-repaired” are shown in the SchValidationLog table, and in the Validation Errors table when you click View Errors for the Repair Database function.</p> <p>No action is required on your part.</p>
inform: pending-repair	<p>The validation test results in an anomaly that is deemed to be harmful to the upgrade process, but one that will be programmatically repaired during the upgrade process.</p> <p>Missing or modified objects are flagged with a status of “inform: pending-repair” in the SchValidationLog table. An example of this type of anomaly is a missing index or a missing primary key constraint. The missing index or primary key constraint will be created correctly, if it does not exist.</p> <p>No action is required on your part.</p>

**Table 6-2 Validation ErrorLevels (continued)**

ErrorLevel	Description
inform: pending-removal	<p>The validation test detected an unrecognized database object that touches a Service Catalog table. The existence of this object may prevent the upgrade from completing successfully. These unrecognized objects are flagged with a status of “inform: pending-repair” in the SchValidationLog table.</p> <p>For example, the following objects (if they exist) are flagged for removal: a) an unrecognized index on a Service Catalog table, b) an unrecognized trigger on a Service Catalog table, c) an unrecognized constraint on a Service Catalog table, and d) an unrecognized foreign key constraint that points to a Service Catalog table. These objects are automatically deleted.</p> <p>No action is required on your part.</p>
error	<p>A validation test has resulted in a hard “error” that cannot be fixed programmatically. Usually, this type of error is related to a bad data relationship, such as missing row, or duplicate entries.</p> <p>All validation entries with ErrorLevel= “error” are shown in the SchValidationLog table, and in the Validation Errors table, when you click View Errors for the Validate Schema or Validate Data function.</p> <p>The TestType column indicates the type of error, and the TestDetail column contains the SQL statement that was used for the validation test. This SQL statement should provide you with some hints regarding the error. This error would cause the upgrade to fail; thus, when such an error is detected, it must be fixed before proceeding with the upgrade.</p> <p><b>The application administrator or database administrator must manually fix all errors of this type, and then run the same Validate function again until it reports no more errors.</b></p> <p>Contact the Cisco Technical Assistance Center (TAC) if you need assistance on how to fix validation errors. In some cases, the RepairScript column may contain a <i>suggested</i> SQL statement that can be used to fix the error. Consult with your application administrator or DBA to ensure that such a repair script is applicable for your specific situation.</p> <p>Document clearly how each validation error is fixed. You will need your notes when you have to repeat the upgrade procedures on another environment.</p>

As described in [Table 6-2](#) above, only validation entries with ErrorLevel= “error”, as shown in the Validation Errors table when you click View Errors for the Validate Schema or Validate Data function, must be manually fixed. All other validation errors, reported in the SchValidationLog table, are automatically handled.

After you manually fix all validation entries with ErrorLevel= “error”, click the same Validate function again to verify that no more errors are reported. It is possible that as a result of your manual fixes, new validation errors may appear. If this happens, you have to repeat the Validate function again, and fix the validation errors, iteratively.

We recommend that you review and address validation errors by doing so iteratively first for all schema validation errors, and then for all data validation errors. This methodology reduces the chance of regression errors you may encounter by mixing schema validation error fixes with data validation error fixes.

### SchValidationLog Table

The results for all validation scripts, regardless of whether validation errors were found or not, are stored in a table called SchValidationLog in the database.

To view the SchValidationLog table:

**Step 1** Connect to your database as the schema owner (that is, CPSCUser), and browse the table SchValidationLog to view the validation results. You can use a utility like SQL Analyzer (Figure 6-2) or SQL\*Plus to connect to your database.

**Figure 6-2 Browse SchValidationLog Table**

SchFunctions	dbo	User	11/5/2007 5:28:25 PM
SchIndColumns	dbo	User	11/5/2007 5:28:25 PM
SchIndexes	dbo	User	11/5/2007 5:28:25 PM
SchObjectActionLog	dbo	User	11/5/2007 5:28:25 PM
SchObjectExceptions	dbo	User	11/5/2007 5:28:25 PM
SchPackages	dbo	User	11/5/2007 5:28:25 PM
SchPrimaryKeys	dbo	User	11/5/2007 5:28:25 PM
SchProcedures	dbo	User	11/5/2007 5:28:25 PM
SchSequences	dbo	User	11/5/2007 5:28:25 PM
SchTabColumns	dbo	User	11/5/2007 5:28:25 PM
SchTables	dbo	User	11/5/2007 5:28:25 PM
SchTriggers	dbo	User	11/5/2007 5:28:25 PM
SchValidationLog	dbo	User	11/5/2007 5:28:25 PM
SchValidationRunAttributes	dbo	User	11/5/2007 5:28:25 PM
SchViewColumns	dbo	User	11/5/2007 5:28:25 PM
SchViews	dbo	User	11/5/2007 5:28:25 PM

**Step 2** Open the SchValidationLog table to view its contents (Figure 6-3).

**Figure 6-3 SchValidationLog Contents**

RunType	TestType	ObjectType	ObjectName	ObjectShortName	ErrorLevel	TestDetail
Check Schema	Table column ty...	Column	DirProject.Perce...	DirProject.Perce...	inform	Expected type: ...
Check Schema	Table column siz...	Column	DirPerson.SSN	DirPerson.SSN	inform	Expected type: ...
Check Schema	Unexpected tabl...	Table	CUSTOMER_TAB...	CUSTOMER_TAB...	inform	NULL
Check Schema	Unexpected tabl...	Table	CUSTOMER_TAB...	CUSTOMER_TAB...	inform	NULL
Check Schema	Unexpected tabl...	Table Column	DirPermission.C...	DirPermission.C...	inform	NULL
Check Schema	Unexpected tabl...	Table Column	DirPerson.CUST...	DirPerson.CUST...	inform	NULL
Check Schema	Unexpected FK ...	FK	FK_CUSTOMER_...	Table name: CU...	pending removal	NULL
Check Schema	Expected index ...	Index	TxInvocationAtt...	TxInvocationAtt...	inform;pending-r...	NULL
Check Schema	Expected index ...	Index	TxObjectRelatio...	TxObjectRelation3	inform;pending-r...	NULL
Check Schema	Expected index ...	Index	TxSatisfaction.T...	TxSatisfaction1	inform;pending-r...	NULL
Check Schema	Expected index ...	Index	XtrAgent.XtrAge...	XtrAgent3	inform;pending-r...	NULL

**Step 3** Check the ErrorLevel column in the SchValidationLog table for the following values and take the recommended actions.

**Step 4** Your SchValidationLog table may contain a lot of entries. Thus, you may want to use the following SQL command to filter the contents:

```
SELECT * FROM SchValidationLog WHERE ErrorLevel= "error"
AND RunType= "Check Data";
```

Include the WHERE clause "ErrorLevel= 'error'" if you just want to see the validation errors that you must fix manually before you can proceed with the upgrade process. Exclude that WHERE clause, or change the value "error" to another value (such as "inform: auto-repairable"; see Table 6-2 for more information) if you want to view other entries in the SchValidationLog table.

Notes about the RunType column in the SchValidationLog table:

- Validate Schema inserts entries with RunType= “Check Schema”.
- Validate Data inserts entries with RunType= “Check Data”.
- Repair Database updates all entries with ErrorLevel= “inform: auto-repairable” to ErrorLevel= “inform: auto-repaired”, and at the same type, changes the RunType to “Fix Data”.

## Validating Schema

Perform the following steps to validate schema:

**Step 1** Click **Validate Schema**.

If the schema validation test completes without validation errors, a “Completed” message appears.

If no errors are reported, proceed to the [Validating Data](#).

If the schema validation test completes with validation errors, a “Completed with errors” message appears.

**Step 2** Click **View Errors**.

The Validation Errors window appears. Resize the window to see the complete table, as shown in the example below ([Figure 6-4](#)).

**Figure 6-4** Validation Errors (Validate Schema)

Error Level	Test Type	Object Type	Test Detail	Object Short Name	Runtime Timestamp
error	Invalid data relationship	ColConstraint	SELECT * FROM DefService WHERE AreaID IS NOT NULL AND NOT EXISTS (SELECT AreaID FROM DefArea DefArea2 WHERE DefArea2.AreaID = DefService.AreaID)	FK_DefS_DefArea	2012-07-18 18:15:46.233

**Step 3** You need to manually fix the errors shown in the Validation Errors table before continuing the upgrade process. See the [Validating Database](#) for more information.

**Step 4** When all validation errors have been fixed iteratively, proceed to the [Validating Data](#) section below.

## Validating Data

Perform the following steps to validate data:

**Step 1** Click **Validate Data**.

If the data validation test completes without validation errors, a “Completed” message appears.

If no errors are reported, proceed to the [Repairing the Database](#).

If the data validation encounters validation errors, then a “Completed with errors” message appears.

**Step 2** Click **View Errors**.

The Validation Errors window appears.

**Step 3** You need to manually fix the errors shown in the Validation Errors table before continuing the upgrade process. See the [Validating Database](#) for more information.

**Step 4** When all validation errors have been fixed iteratively, proceed to the [Repairing the Database](#) section below.

---

## Repairing the Database

Perform the following steps to repair the database:

**Step 1** Click **Repair Database**.

When the database has been repaired a “Completed” message appears,

**Step 2** (Optional) Click **View Errors**.

The Validation Errors window appears. Resize the window to see the complete table.

Note that the Validation Errors are only with ErrorLevel= “inform:auto-repaired” that are fixed programmatically by the Repair Database function.

**Step 3** Proceed to the [Completing Installation](#) section below.

---

## Completing Installation

You have validated and repaired your database, and are now ready to proceed with the upgrade.

**Step 1** Click **Next** to proceed to the next page of the Service Catalog installation wizard.


**Step 2** Continue to run the installation wizard as described in the [Installing Prime Service Catalog on WildFly Application Server](#) or [Installing Prime Service Catalog on WebLogic Application Server](#).

When you click **Install** on the Pre-Installation Summary page of the installation wizard, the installer proceeds to execute the upgrade scripts to modify your database schema and contents. Depending on the size of your database, the upgrade scripts may take a long time to run. After the upgrade scripts modify the database schema and contents, the installer proceeds to create the WAR files. Follow the same procedures described in [Postinstallation Tasks for WildFly](#) section or [Postinstallation Configuration for WebLogic](#) section to deploy the WAR files for the Service Catalog product.


- Step 3** Once you finish the deployment of the WAR files, and are able to start up the application servers, you have essentially completed the upgrade process. Your Service Catalog application is now at Release 12.1. At this time, if you wish, you can take a backup of the databases and the installation directory. If you are using Oracle DBMS, it is recommended that you again execute recompile statistics for the upgraded databases in order to improve the system runtime performance.

## Performing Post-upgrade Tasks

To perform post-upgrade tasks:

- Step 1** Where necessary, recreate custom database objects that were deleted from the database by the installer.
- Step 2** Any custom code must be compatible with the new version of the JDK:
- Service Link custom adapters must be rebuilt with Release 12.1 version of the Service Link ADK.
  - Custom Java code developed at the customer site must be rebuilt using the new JDK.
  - Any enterprise portal into which Service Catalog Portlets are deployed must use JDK 8 Update 91.
- Step 3** Service Import/Export is not backward compatible with previous releases. Services exported in prior releases cannot be imported into Release 12.1. If you have maintained any Services export files in a code repository prior to upgrade, then you may want to export them again, and mark them for Release 12.1.
-  **Note** Users imported from a different database (for example, using Catalog Deployer) must reset their passwords for logging into the application. This is because the Key Encryption Key is different for different databases.
- Step 4** Follow procedures your organization has used in the past to re-implement all customizations for the application.
- Step 5** Connect to the Service Catalog application as an administrative user. Navigate to the “Administration” module, and click the **Settings** tab. Under Customizations Settings, look for “Browser Cache” (as shown in [Figure 6-5](#)).

**Figure 6-5 Enable Browser Cache Setting**

Browser Cache:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	The Browser Cache setting enables the browser-side caching of images, javascripts, css, etc., which may improve performance. When the Version setting value is incremented, the login process is interrupted until the browser's cache is deleted. Default is Disabled.
Version:	2 	
<input type="button" value="Update"/>		

361973

- Step 6** Click the **Enabled** radio button for the “Browser Cache” setting. Click the + button located to the right of the Version text box. This will increment the Version number by one. Then click **Update**. This setting will notify the users to clear their browser cache when they connect to the Service Catalog URL for the first time after the Service Catalog system is upgraded.
- Step 7** The master key password files kek\_new.txt and kek\_old.txt, located under the <ServiceCatalog\_Install\_Dir>/dist directory, must be backed-up to a secure location.



- Step 8** After the Audit Log data has been migrated, disable the Change Data Capture feature provided by the database vendor, as Prime Service Catalog 12.1 no longer uses this feature.
- Disable the Change Data Capture for an SQL Server by executing the following stored procedure:  
`sp_DisableCDC()`
  - In Oracle 12c, delete the CDCADMIN schema.
- 

## Moving Customizations to Website

The Custom Themes for Service Catalog module is no longer supported and the only way to customize Service Catalog is through website model. If you have customizations applied on Service Catalog module prior to 12.1 you would need to move the customization files to a new location during upgrade. The *ngc* folder which contained all the UI files is now removed from the location `/RequestCenter/modules/`. The files used for customization found in `/custom/*` folders must now be moved to the out-of-box or custom website folders.

To facilitate the transition from the Classic Custom Themes to the new website model, two scripts are provided. These scripts can be used to change the references to the *ngc* folder in the custom files to `ServiceCatalogWebsite` or any other website directory. This would make it easy to move the files out of classic custom to website.

### High-Level Steps to Migrate to Website Model:

---

- Step 1** Download the files available on [cisco.com](http://cisco.com).
- Step 2** Navigate to the directory that contains the downloaded `WebsiteModelUpgradeScripts.zip` and extract the files.
- Step 3** Run the `GenerateCSV.py` script. For detailed info on this script, see section [Working of Script GenerateCSV.py, page 6-17](#).
- Step 4** Review the output `.csv` file generated from the `GenerateCSV.py` script. You may need to update the paths, if necessary.
- Step 5** Run the script `ChangePathReferences.py`, which updates the paths referring to old *ngc* folder to `ServiceCatalogWebsite` folders specified in the input file. For detailed info on this script, see section [Working of Script ChangePathReferences.py, page 6-18](#).
- 

### Working of Script GenerateCSV.py

This script generates a report of all the customization files in which path references need to be modified. The script parses the files given in the input file and looks for matching strings from the list of predefined regexs (references to old *ngc* folder) and the additional regexs (new references) given as user inputs, if any. The pre-defined regexs take priority over the additional regexs. These matches are written in the output file along with a suggested reference.

1. In case of pre-defined regex matches, the 'suggested reference' column is automatically populated.
2. In case new regexs are given as input, the match is replaced with 'replace\_this' string in the suggested reference column.

**Input:**

1. .txt file with file paths
2. .txt file with additional regexes, if any (can be left empty)
3. Folder path to generate the output file

**Output:**

This script generates a .csv file with the below columns in the destination folder. The table represents the fields in the output file with an example.

File moved	String Matched	Referred in file	Line numbers	Current Reference	Suggested reference
Add.png		/RC/modules/idp/APIManager.js		../../ngc/img/add.png	/RC/website/common/images/add.png

**Note**

You must thoroughly review the output before you proceed to run the script `ChangePathReferences.py`. Review the suggested references column and change them, if needed.

**Working of Script ChangePathReferences.py**

This script uses the .csv output file generated from the script `GenerateCSV.py` and ‘reads’ the columns *Referred in file*, *Current Reference*, and *Suggested reference*. The script then replaces the *Current References* path with the *Suggested References* in the respective files.

**Input:**

The .csv output file generated by the first script (with changes, if any).

**Result:**

All the references in custom files to the files in *ngc* folder are now changed to the file paths from website folder.

The next chapter describes the procedures for upgrading the Cognos component of the Reporting module. If your preupgrade Service Catalog system included the Reporting module, then you must continue with the next chapter to complete the upgrade process for the Cognos component so that the Reporting module will work for Release 12.1.



## Installing and Upgrading Reporting Module

---

This chapter describes how to install the Reporting module, and to use the various installer utilities developed by Cisco to install the Cognos software components and integrate them with the Cisco Prime Service Catalog application.

Cognos environment is comprised of an application server and a database server.

- An application server is the computer where you install the IBM Cognos software, and execute the configuration scripts to integrate Cognos with the Cisco Prime Service Catalog application.
- A database server is the computer where the Data Mart and Content Store databases reside.

The following sections describe the prerequisites for the Cognos application server and database server.

### Prerequisites for Installing Reporting

#### Cognos Application Server Requirements

##### Operating Systems

- IBM Cognos software must be installed on a computer that runs Windows Server 2012 R2 (64-bit) operating system.
- It is recommended but not required that the Cognos application server is a separate computer from the Cisco Prime Service Catalog application. However, if the Cisco Prime Service Catalog application is running on a Linux computer, then the Cognos application server must be a separate machine with the Windows operating system.

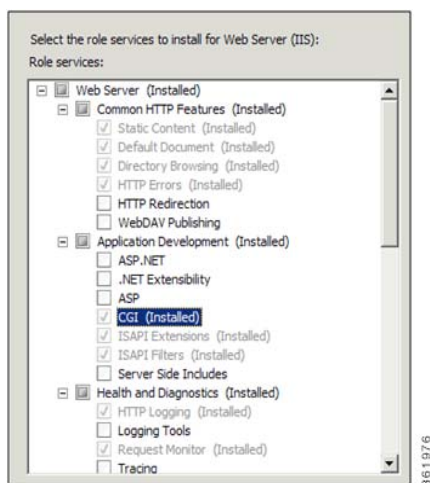
##### Memory and Disk Space

- The application server must have at least 8 GB RAM and 50 GB of free disk space.
- There must be at least 2 GB of free disk space on the drive that contains the %TEMP% directory, if this is different from the drive when you plan to install the Cognos software.

## Internet Information Services (IIS)

- The “Web Server (IIS)” role must be installed on the Cognos application server.
- The “World Wide Web Publishing Service” is configured to start up automatically.
- IIS must have a site named “Default Web Site”.
- The following role services must be enabled for IIS:
  - CGI
  - ISAPI Extensions
  - ISAPI Filters

**Figure 7-1** Select Role Services for Web Server



## Internet Explorer

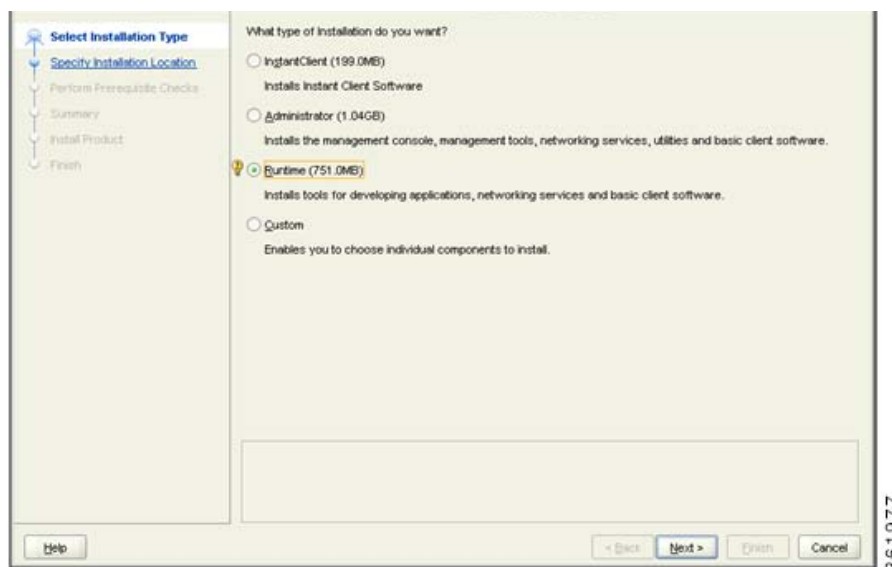
- Microsoft Internet Explorer (IE) version 11 and FireFox 49.0.2.xesr (or later) are supported. Use IE11, FireFox 49.0.x esr browser when accessing the Cognos UI or the “Advanced Reporting” module inside of the Cisco Prime Service Catalog.
- The following browser settings must be enabled:
  - Accept third-party cookies
  - JavaScript
  - Run ActiveX controls and plug-ins
  - Script ActiveX controls marked safe for scripting
  - Active scripting
  - Allow META REFRESH

## Database Client Connectivity

The appropriate Database Client Connectivity software must be installed on the Cognos application server, and preconfigured to connect to all three databases: Request Center database, Data Mart database, and Content Store database.

- **For Oracle 12c:** The Oracle Client 12.1.0.2(32-bit) software is required (note that the 32-bit version of Oracle 12c Client software must be used, even though the Windows Server 2012 R2 operating system is a 64-bit version). The Cognos software installation is not bundled with the necessary JDBC driver to connect to an Oracle database. Thus, if the Content Store database is on Oracle, you must install the Oracle Client software on the Cognos application server. When installing Oracle Client 12.1.0.2, choose the “Runtime” option:

**Figure 7-2** Select Installation Type



- **For Microsoft SQL Server 2012 SP3 or 2016:** The SQL Server Client Connectivity software is not required. The Cognos installation is already bundled with the necessary JDBC driver to connect to the SQL Server database server.

## Other Requirements

- You must log in as a user with administrative privileges on the application server to install the Cognos software. This user must also have read and write permission to the %TEMP% directory.
- The following machines must all be set to the same timezone:
  - The Cisco Prime Service Catalog application server
  - The Cognos application server
  - The database server where the following databases reside: Service Catalog, Data Mart, and Content Store

- A domain name system (DNS) should have been configured for the computer. The Primary DNS suffix of the hostname must be assigned to an appropriate value (for example, *mydomain.com*) and the hostname should resolve to the fully qualified domain name (for example, “ping *myserver*” should resolve to *myserver.mydomain.com*).
- The Service Catalog application server and the Cognos application server must belong in the same domain. For example, if the Service Catalog application server was installed on a computer in the domain called *mydomain.com*, then the Cognos application server must also belong in the same domain *mydomain.com*.
- Throughout this installation process, whenever you have to enter a host name or a server name, you must enter it as a fully qualified domain name. For example, do not enter “*localhost*,” or “*cognosserver*”; instead, enter “*cognosserver.mydomain.com*”. When you connect to Service Catalog, you must also enter the fully qualified domain name in the URL, for example, *http://servicecatalog.mydomain.com/RequestCenter*.
- Throughout this installation process, whenever you open a Command Prompt window to execute any script, make sure you increase the Command History Buffer Size (to something like 999) so that you can view the entire output on the Command Prompt window. Not all output is captured in the installation log file.

## Cognos Database Server Requirements

The Reporting module requires access to three databases:

- The Service Catalog database
- The Data Mart database
- The Content Store database

In addition to the Service Catalog database, the Reporting module requires two more databases, Data Mart and Content Store. The next section describes how to create the Data Mart and Content Store database on either Oracle 12c or SQL Server 2012 SP3 or 2016.

The Data Mart and Content Store database must be on the same type and version of RDBMS as the Service Catalog database. For example, if the Service Catalog database is on Oracle 12c, then the Data Mart and Content Store databases must also be created on Oracle 12c. If the Service Catalog database is on SQL Server 2012 SP3 or 2016, then the Data Mart and Content Store databases must also be created on respective version of SQL Server.

The database server must be configured to support TCP/IP protocol for client connectivity, and must be accessible from the Cognos application server.

The database administrator must back up the Data Mart and Content Store database regularly because they contain all of the Cognos data, including custom reports and views as well as saved reports. To ensure the security and integrity of the databases, it is also important to protect the databases from unauthorized or inappropriate access.

## Creating Data Mart and Content Store Databases for Oracle

For a new installation, you can prepare the tablespaces and users for the Data Mart and Content Store databases manually as described in this section before executing the Reporting installer, or you can let the Reporting installer create the database users on the default tablespaces for you by selecting the "Create Database" option presented by the installation wizard. The "Create Database" option of the Reporting installer is described in more detail in the "Installing Reporting" section.

To create tablespace and users for the Data Mart and Content Store database:

- Step 1** The Oracle database must be configured to use a Unicode character set (that is, either UTF-8 or UTF-16). To determine if the database character set is Unicode, execute the following sql command:

```
SELECT VALUE FROM NLS_DATABASE_PARAMETERS WHERE PARAMETER='NLS_CHARACTERSET';
```

If the returned value for the NLS\_CHARACTERSET parameter is either AL32UTF8 or AL16UTF16, then your Oracle database supports Unicode. Otherwise, you need to create a new Oracle database, and specify the character set to be either AL32UTF8 or AL16UTF16 at creation time.

- Step 2** The ORACLE parameter CURSOR\_SHARING must be set to EXACT and the parameter PROCESSES must be set to 500 (or higher). Execute the following commands to find out the current values of CURSOR\_SHARING and PROCESSES:

```
SHOW PARAMETER CURSOR_SHARING;
```

```
SHOW PARAMETERS PROCESSES;
```

- Step 3** If CURSOR\_SHARING is not set to EXACT, you can use the following command to change it:

```
ALTER SYSTEM SET CURSOR_SHARING=EXACT SCOPE=BOTH SID='*';
```

- Step 4** If the PROCESSES and SESSION parameters are smaller than 600, then work with your DBA to bump up these parameters for your Oracle database to 600 (or higher).

- Step 5** Create a new tablespace named DATAMART, with initial size of 500 MB and AUTOEXTEND ON.

- Step 6** Create a new temporary tablespace named DATAMART\_TEMP, with initial size of 30 MB and AUTOEXTEND ON.

- Step 7** Create a database user named DMUser, with default tablespace set to DATAMART and temporary tablespace set to DATAMART\_TEMP. DMUser should be granted QUOTA UNLIMITED on the DATAMART tablespace. DMUser will be the owner of the Data Mart schema.

- Step 8** Grant the following permissions to DMUser:

```
GRANT
  CREATE SESSION,
  CREATE TABLE,
  CREATE PROCEDURE,
  CREATE SEQUENCE,
  CREATE TRIGGER,
  CREATE VIEW,
  CREATE MATERIALIZED VIEW,
  CREATE SYNONYM,
  ALTER SESSION
  TO DMUser;
```

- Step 9** Create another database user named CSUser, with default tablespace set to DATAMART and temporary tablespace set to DATAMART\_TEMP. CSUser should be granted QUOTA UNLIMITED on the DATAMART tablespace. CSUser will be the owner of the Content Store schema.

- Step 10** Grant the following permissions to CSUser:

```
GRANT
  CREATE SESSION,
  CREATE TABLE,
  CREATE PROCEDURE,
  CREATE SEQUENCE,
  CREATE TRIGGER,
```

```
CREATE VIEW
TO CSUser;
```

## Creating Data Mart and Content Store Databases for MS SQL Server

For new installation, you can prepare the Data Mart and Content Store databases and login users as described in this section before executing the Reporting installer, or you can let the Reporting installer create the databases and login users for you by selecting the "Create Database" option presented by the installation wizard. The "Create Database" option of the Reporting installer is described in more detail in the "Installing Reporting" section.

To create the Data Mart and Content Store databases and login users:

- 
- Step 1** SQL Server can be installed as Default Instance or a Named Instance.
  - Step 2** SQL Server must be configured with mixed-mode authentication (that is, allows both SQL Server authentication and Windows authentication).
  - Step 3** Create two separate databases called "Datamart" and "ContentStore", each with initial size of 500 MB and autogrowth by 10 percent. The collating sequence of each database must be case-insensitive.
  - Step 4** Create two separate database login accounts named "DMUser" and "CSUser".



### Note

DMUser and CSUser must be SQL Server login accounts that authenticate to the SQL Server using SQL Server authentication method, and not Windows authentication method.

- 
- Step 5** Assign the database user account "DMUser" as the db\_owner of the "Datamart" database. Verify your settings to ensure that a) the user "DMUser" in the Data Mart database is mapped to the login account "DMUser" in the SQL Server, b) the default schema is "dbo", and c) the user "DMUser" has the "db\_owner" database role membership.
  - Step 6** Assign the database user account "CSUser" as the db\_owner of the "ContentStore" database. Verify your settings to ensure that a) the user "CSUser" in the Content Store database is mapped to the login account "CSUser" in the SQL Server, b) the default schema is "dbo", and c) the user "CSUser" has the "db\_owner" database role membership.
- 

## Sizing the Content Store Database

The size of the Content Store database depends on a number of factors:

- Number of concurrent users
- Number of saved reports (plus number of pages/rows/images per report)
- Number of saved report views (plus number of pages/rows per report)
- Format of the reports (PDF, HTML, and so on)

The following guidelines, adapted from an article published in the Cognos Knowledge Base, may help you estimate database sizing requirement, based on usage estimates from the above parameters.

Content Store sizing is a function of:



- System space: transaction logs; Cognos estimates 3,000,000 KB for a database with 250 active users.
- Temporary space: required to generate reports; estimate 100,000 KB per concurrent user.
- Data space: required to hold reports and views saved by users; user folders; and the Framework Manager models on which the reports are based.
- The total number of saved reports and views is a major factor in terms of Content Store sizing, and the most difficult to predict. This can be partially controlled by Cognos Administrators limiting the number of versions of a report that can be saved by each user.
- The size of each saved report is based on the number of report pages. Factors that may influence the average size of a report include number of pages; formatting and text selection; and the inclusion of images. Cognos estimates that following requirements for saved objects which users may create.
- Cognos also estimates the number of each of these saved objects that a “typical” user is likely to maintain. Multiplying these numbers by the storage requirements for each object yields an estimate for volume- (user-)dependent storage requirements for data space within the Content Store.

Object	Storage Requirements (Estimate)	# Per User
Saved Report, PDF format, 1–10 pages	340 KB	2
Saved Report, PDF format, 10–100 pages	440 KB	9
Saved View, 1–100 rows	250 KB	3
Saved View, 100–1000 rows	350 KB	8
Schedule (daily or weekly)	30 KB	2

- You need only multiply these requirements by the number of Cognos users to estimate this most volatile aspect of disk usage.

## Installing Cognos Software

This section describes how to install Cognos 10.2.1.



### Note

You must log in as a user with administrative privileges to perform the installation tasks described in this section.

## Downloading Cognos Software

Perform the following tasks to download Cognos software:

- Step 1** Access the Cisco product download web site and authenticate with the user name and password provided to you.
- Step 2** Search for the product name “Cisco Prime Service Catalog Reporting”, or navigate within the product selector to locate the Cognos Business Intelligence installer and fixed packs.

- Step 3** Choose **Business Intelligence Install** and download the following files under version 10.2.1 to your Cognos application server machine:

File to download	Description
bi_svr_64b_10.2.1_win_ml.tar.gz	Cognos 10.2.1 Business Intelligence Server (64-bit)
bi_dmgr_64b_10.2.1_win_en.tar.gz	Cognos 10.2.1 Data Manager (64-bit)
up_bisrvr_winx64h_10.2.5002.78_ml.tar.gz	FixPack2 for Cognos 10.2.1

- Step 4** Extract the Cognos Business Intelligence Server zip file into a temporary directory such as C:\cognos\_bi\_software. Extract the Cognos Data Manager zip file into a temporary directory such as C:\cognos\_dm\_software. Extract the Cognos FixPack zip file into a temporary directory such as C:\cognos\_fixpack.
- Step 5** Delete the JAVA\_HOME environment variable, if it exists on the Cognos machine. This is because Cognos installation program will use its embedded Java, which may conflict with the version of Java defined for JAVA\_HOME environment variable. After you install Cognos software, you will then set the JAVA\_HOME environment variable to point to the Java directory under the Cognos installation directory.

## Installing Cognos Business Intelligence Server

Perform the following tasks to install Cognos business intelligence server:

- Step 1** (Assuming that you extracted the Cognos BI software under the C:\cognos\_bi\_software directory) Open the folder C:\cognos\_bi\_software\winx64h.
- Step 2** Double-click **issetup.exe** to launch the Cognos Setup program.
- Step 3** Walk through the installation wizard by choosing all default values presented on the screen, until you get to the Component Selection screen.
- Step 4** Choose only the following components, and deselect all other components:
- Application Tier Components
  - Gateway
  - Content Manager
- Step 5** Click **Next** and proceed with the rest of the installation wizard, until you get to the Finish screen.
- Step 6** Uncheck the “Start IBM Cognos Configuration” option, and then click **Finish**.

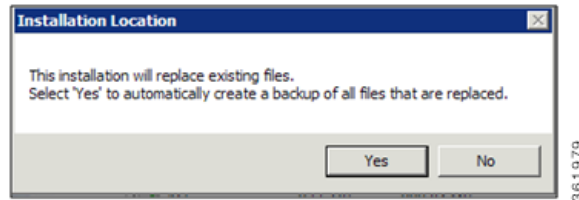
## Installing Cognos Data Manager

Perform the following steps to install Cognos data manager:

- Step 1** Go to C:\cognos\_dm\_software\winx64h directory (assuming that the Cognos Data Manager software is extracted to this location).
- Step 2** Double-click **issetup.exe** to launch the Cognos Setup program.

- Step 3** Walk through the installation wizard by choosing all default values presented on the screen, until you get to the Installation Location screen.
- Step 4** Enter the same folder name where you have installed the Cognos Business Intelligence Server (for example, C:\Program Files\cognos\c10\_64). Then click **Next**.
- Step 5** If you see the message “Warning: You are installing to the same location as a previous installation. Do you want to continue?”, click **Yes** to proceed.
- Step 6** If the following message appears, click **No** to proceed:

**Figure 7-3** Installation Location Warning Message



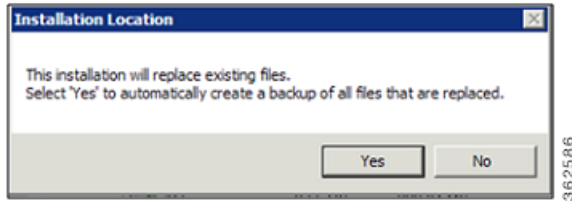
- Step 7** When the Component Selection screen appears, choose only the following component, and deselect all other components:
- Data Manager Engine
- Step 8** Click **Next** and proceed with the rest of the installation wizard, until you get to the Finish screen.
- Step 9** Uncheck the “Start IBM Cognos Configuration” option, and then click **Finish**.

## Installing Cognos Fix Pack

Perform the following steps to install Cognos fix pack:

- Step 1** Assuming that you extracted the Cognos software under the C:\cognos\_fixpack folder, go to the folder "C:\cognos\_fixpack\winx64h".
- Step 2** Double-click **issetup.exe** to launch the Cognos Setup program.
- Step 3** Walk through the installation wizard by choosing all default values, until you get to the Installation Location screen.
- Step 4** Enter the same folder name where you have installed the Cognos Business Intelligence Server (for example, C:\Program Files \cognos\c10\_64). Click **Next**.
- Step 5** If the following message appears, click **No** to proceed:

**Figure 7-4** Installation Location Warning Message



- Step 6** Click **Next** and proceed with the rest of the installation wizard, until you get to the Finish screen.
- Step 7** Click **Finish**.

## Installing Reporting

This section describes how to install and configure Cisco Prime Service Catalog Reporting. You must log in as a user with administrative privileges to perform the installation tasks described in this section.



### Note

Reporting Installer uses the Cognos in-built JRE 7 and you must not have the Oracle JDK 1.8 or 1.7 installed on the same system.

## Executing Reporting Setup

Reporting is installed by running a setup program which installs and launches an installation wizard.

To execute the setup program:

- Step 1** On the Cognos machine, set or modify the JAVA\_HOME environment variable to "<COGNOS\_HOME>\bin64\jre\7.0", where <COGNOS\_HOME> is the installation directory for Cognos (i.e. C:\Program Files\cognos\c10\_64). Then, add "%JAVA\_HOME%\bin" to the beginning of the PATH environment variable. This will ensure that the Java executable under <COGNOS\_HOME>\bin64\jre\7.0\bin will be used.
- Step 2** Copy the unlimited strength JCE policy files from <Build\_No>\reporting\ibm\_jre\_7.0\_policy to the %JAVA\_HOME%\jre\lib\security directory, overwriting the existing files. The unlimited strength policy files are "local\_policy.jar" and "US\_export\_policy.jar".
- Step 3** Extract the Cisco Prime Service Catalog software that you downloaded from the Cisco web site to your computer, if you have not already done so.
- Step 4** Double-click **reporting\_setup.cmd** to launch the installation wizard.
- A progress bar appears, when complete, the first page of the installation wizard appears.

## How to Use the Installation Wizard

The installation configuration options are case-sensitive, so ensure that you enter a value, such as a database name or a JMS queue name, with case sensitivity; otherwise, your installation may fail.

## Running the Reporting Installation Wizard

This section provides instructions for running the Reporting installation wizard.

### Prerequisite

Copy the `kek_new.txt` and `kek_old.txt` files from the `<ServiceCatalog_Install_Dir>\dist` directory to `C:\temp` or any other folder on the reporting machine. During the installation, you will be prompted for the master key file and you must navigate to this path in that window and select the `kek_new.txt` file.

- 
- Step 1** Stop the IIS web server.
  - Step 2** Launch the installation wizard (see [Executing Reporting Setup](#)).
  - Step 3** On the first page of the installation wizard, click **Next** to begin.
  - Step 4** On the Choose Install Folder panel, enter a destination folder for the installation and click **Next**.  
The default destination folder is “`C:\CiscoPrimeServiceCatalog`”. If desired, enter a different destination folder, or click Choose to locate and select another folder (or create a new one). The path name for the destination folder must not contain any spaces. Throughout this document, this destination folder is referred to as `<Reporting_Install_Dir >`.
  - Step 5** Enter the Cognos root directory. This is where you installed the Cognos 10.2.1 software. The default Cognos root directory is “`C:\Program Files\ibm\cognos\c10_64`”. If needed, enter a different root directory, or click Browse to locate and choose the directory. Click **Next**.
  - Step 6** In the Database Selection panel, choose the database platform (Microsoft SQL Server or Oracle) and click **Next**.  
Refer to your [Database Information Worksheet](#) that you filled out earlier to determine your database platform.

- Step 7** In the Service Catalog Database panel, enter your Service Catalog database configuration values. For more information on updating the values on the Service Catalog Database panel, see [Table 7-1](#). Use your [Database Information Worksheet](#) that you filled out earlier to help you determine what configuration values to enter.

**Table 7-1 Request Center Database Table for Reporting**

Field	SQL Server	Oracle Server
Host IP Address	Enter the IP address of the server where the Service Catalog database resides.	Enter the IP address of the server where the Service Catalog schema resides.  When using Oracle RAC use Scan IP Address only.
Port	Enter the TCP/IP Port Number used by your Database Server. Valid port numbers are from 1 to 65535. The default value is 1433.	Enter the TCP/IP Port Number used by the Database Server. The default value is 1521.
Database Name	Enter the name of the RequestCenter database. By default, the value is "Service Catalog". Enter only alphanumeric characters. Do not use any space characters.	Not Applicable
Database SID or Database Service Name	Not Applicable	If you use SID to connect to your Oracle database, then select the SID radio button, and enter the Oracle SID value. If you use Service Name to connect to your Oracle database, then select the Service Name radio button, and enter the Service Name value.  When using Oracle RAC use the Service Name only.
Username	Enter the database username. Enter only alphanumeric characters. Do not include any space characters. This username is the login ID and the db_owner of the "Service Catalog" database. The default value is "CPSCUser".	Enter the database username. Enter only alphanumeric characters. Do not include any space characters. This username is the login ID and schema name for the database schema. The default value is "CPSCUser".
Password	Enter the password for the Database Username.	Enter the password for the Database Username.

- Step 8** Click **Next** to proceed to the next page of the wizard.

The installer performs a connection test to your Service Catalog database using the configuration values you entered and checks that the prerequisites for your database platform have been fulfilled.

If the database connection test fails, a "Database Test Connection Failed" dialog box message appears. If you get this message, click **OK** to close the dialog box, and make any necessary modifications to the information on the Service Catalog Database panel. If you want to abort the installation wizard at this point, click **Cancel**.

If the database connection test passes, the Master Key File panel appears.

**Step 9** In the Master Key File panel, enter (or browse to) the full path to the kek\_new.txt file that you copied to C:\Temp earlier.

**Step 10** Click Next.

The Prime Service Catalog installer will verify that the master key in the specified kek\_new.txt file matches with the Service Catalog database that you entered in the last panel. If the master key file does not match, the installer will raise an error and will not let you proceed to the next step.

**Step 11** In the DataMart Database Creation panel:

- If you have already created your database, then select **No** here and click **Next** to continue. You will be prompted for the information of your existing database. Refer to the [Data Mart Database Table for Reporting](#) to enter the database information.
- If you have not created the database in advance, select **Yes** to let the installer create the database for you and click **Next**. You will be prompted for the connection information to your database server so that the installer can create the database on the fly. Enter the database information on the Data Mart Database panel and click **Create Datamart**.

If the database creation is successful, the Data Mart database successful message dialog appears. Click **OK** to close the message dialog box. Refer to the [Data Mart Database Table for Reporting](#) below to enter the database information.

**Note**

---

This "Create Datamart" feature will create a very basic Data Mart database that meets the minimum requirements for the Service Catalog Reporting module to operate. This feature is recommended for a Demo or Test system, but for a Production system, it is advisable that you work with your DBA to create the Data Mart database in advance which meets all of the product requirements as described in the Configuring Databases section, as well as any performance, reliability and security requirements that adhere to your corporate policy.

---

- If you are performing an upgrade installation, then select **No** and click **Next**. You will be prompted to enter the information of your existing Data Mart database. Refer to the Data Mart Database Table for Reporting to enter the database information. Refer to [Chapter 6, “Upgrading Prime Service Catalog”](#) for more detailed information.



**Note** The fields in the Data Mart Database panel varies depending on whether you clicked **Yes** or **No** in the Data Mart Database Creation panel. Use the [Table 7-2](#) accordingly.

**Table 7-2 Data Mart Database Table for Reporting**

Field	SQL Server	Oracle Server
Host IP Address	Enter the IP address of the Database Server.	Enter the IP address of the Database Server. When using Oracle RAC use Scan IP Address only.
Port	Enter the TCP/IP Port Number used by the Database Server. The default value is 1433.	Enter the TCP/IP Port Number used by the Database Server. The default value is 1521.
Database name	Enter the name of the database for the Data Mart. Enter only alphanumeric characters. Do not include any space characters. The default value is "Datamart"	Not Applicable
sa password	To create the database in SQL Server, the installer must connect to SQL Server as the "sa" user. Enter the password for the "sa" user here.	Not Applicable
sys password	Not Applicable	Enter the password for the "sys" user.
Database SID or Database Service Name	Not Applicable	If you use SID to connect to your Oracle database, then select the SID radio button, and enter the Oracle SID value. If you use Service Name to connect to your Oracle database, then select the Service Name radio button, and enter the Service Name value. When using Oracle RAC use the Service Name only.
Username	Enter the database username. Enter only alphanumeric characters. Do not include any space characters. This username will be the login ID and the db_owner of the "Datamart" database. The default value is "DMUser".	Enter the database username. Enter only alphanumeric characters. Do not include any space characters. This username will be the login ID and schema name for the database schema. The default value is "DMUSER".
Password	Enter the password for the Database Username.	Enter the password for the Database Username.



**Table 7-2 Data Mart Database Table for Reporting**

Field	SQL Server	Oracle Server
Confirm Password	Re enter the password for the Database Username.	Re enter the password for the Database Username.
User tablespace	Not Applicable	<b>(Optional value)</b> If you have a specific Oracle tablespace name, enter it here. The default tablespace for the shema will be set to this value.  If you leave this value blank, then the installer will use whatever the default USER tablespace that the Oracle server provides.
Temp tablespace	Not Applicable	<b>(Optional value)</b> If you have a specific Oracle temp tablespace name, enter it here. The temp tablespace for the shema will be set to this value. If you leave this value blank, then the installer will use whatever the default TEMP tablespace that the Oracle server provides.

**Step 12** In the Data Mart Database panel, click the **Next** button to continue. The installer will connect to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if it detects that a certain required database setting is missing. If a database validation error occurs, the installer will not allow you to move on. You can do one of the following:

- a. Close the error dialog and click **Cancel** to exit the installation wizard, or
- b. Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next page.

If the database validation passes, the Content Store Database Creation panel appears.

**Step 13** For a new installation, you can prepare the database in advance as described in the [Cognos Database Server Requirements](#) section.

- If you have already created your database, then select **No** and click **Next** to continue. You will be prompted for the information of your existing database.  
  
Refer to the Content Store Database Table for Reporting below to enter the database information. Click **Next**.
- If you have not created the database in advance, select **Yes** to let the installer create the database for you and click **Next**. You will be prompted for the connection information to your database server so that the installer can create the database on the fly. Enter the database information on the Content Store Database Creation panel and click **Create Content Store**. If the database creation is successful, the Content Store Database successful message dialog will appear.

**Note**

The Create Database feature will create a very basic Content Store database that meets the minimum requirements for the Service Catalog Reporting module to proceed. This feature is recommended for a Demo or Test system, but for a Production system, it is advisable that you work with your DBA to create

the Content Store database in advance which meets all of the product requirements as described in the Cognos Database Server Requirements section, as well as any performance, reliability and security requirements that adhere to your corporate policy.

- If you are performing an upgrade installation, then select **No** and click **Next**. You will be prompted to enter the information of your existing Content Store database. Refer to [Chapter 6, “Upgrading Prime Service Catalog”](#) for more detailed information.

Refer to the [Table 7-3](#) below to enter the database information. Click **Next**.

**Note**

The fields in the Content Store Database panel varies depending on whether you clicked Yes or No in the Content Store Database Creation panel. Use the Content Store Database Table for Reporting accordingly.

**Table 7-3 Content Store Database Table for Reporting**

Field	SQL Server	Oracle Server
Host IP Address	Enter the IP address of the Database Server.	Enter the IP address of the Database Server. When using Oracle RAC use Scan IP Address only.
Port	Enter the TCP/IP Port Number used by the Database Server. The default value is 1433.	Enter the TCP/IP Port Number used by the Database Server. The default value is 1521.
Database name	Enter the name of the database for the Content Store. Enter only alphanumeric characters. Do not include any space characters. The default value is "ContentStore"	Not Applicable
sa password	To create the database in SQL Server, the installer must connect to SQL Server as the "sa" user. Enter the password for the "sa" user here.	Not Applicable
Database SID or Database Service Name	Not Applicable	If you use SID to connect to your Oracle database, then select the SID radio button, and enter the Oracle SID value. If you use Service Name to connect to your Oracle database, then select the Service Name radio button, and enter the Service Name value. When using Oracle RAC use the Service Name only.
Username	Enter the database username. Enter only alphanumeric characters. Do not include any space characters.  This username will be the login ID and the db_owner of the "ContentStore" database. The default value is "CSUser".	Enter the database username. Enter only alphanumeric characters. Do not include any space characters.  This username will be the login ID and schema name for the database schema. The default value is "CSUSER".

**Table 7-3** Content Store Database Table for Reporting

Field	SQL Server	Oracle Server
Password	Enter the password for the Database Username.	Enter the password for the Database Username.
Confirm Password	Re enter the password for the Database Username.	Re enter the password for the Database Username.
User tablespace	Not Applicable	<b>(Optional value)</b> If you have a specific Oracle tablespace name, enter it here. The default tablespace for the shema will be set to this value.  If you leave this value blank, then the installer will use whatever the default USER tablespace that the Oracle server provides.
Temp tablespace	Not Applicable	<b>(Optional value)</b> If you have a specific Oracle temp tablespace name, enter it here. The temp tablespace for the shema will be set to this value. If you leave this value blank, then the installer will use whatever the default TEMP tablespace that the Oracle server provides.

**Step 14** Click the **Next** button on the Content Store Database panel to continue. The installer will connect to the database to validate the required settings for the database. If the installer created the database for you, then it would meet all of the required settings, and the validation test would pass. If you provided the information for an existing database, then the installer may report a validation error if it detects that certain required database setting is missing. If a database validation error occurs, the installer will not allow you to move on. You can do one of the following:

- a. Close the error dialog and click **Cancel** to exit the installation wizard, or
- b. Fix the missing database setting on a separate database connection session. Then come back to this screen, close the error dialog, and click **Next** again. At this point, the installer will repeat the validation test, and if the test passes, it will let you move to the next page.

If the database validation passes, the Content Store Root Directory page appears.

**Step 15** Click **Next** to proceed. The Cognos Settings page appears.

**Step 16** Enter the following information for Cognos server.

- **Cognos Server Name:** Enter the fully qualified domain hostname (not IP address) of the computer where the Cognos software is installed.
- **Configure IIS?:** Do not deselect this option. The installer will automatically configure the Cognos application on the IIS web server on this computer.
- **IIS Web Site:** Do not change the default value of "Default Web Site".

**Step 17** Click the **Advanced Options** button. The Advanced Options dialog box appears.

Specify if you want to execute the database scripts as part of the installation by selecting the **Execute SQL Scripts** checkbox. This checkbox is selected by default.

You should deselect this setting only in exceptional circumstances such as:

- If a separate review of the scripts by internal personnel is required before they execute. In this case, you will need to step through this wizard again, this time selecting the checkbox, in order to execute the scripts and complete the installation.
- A previous installation attempt successfully executed these scripts but failed later during the installation process. In this case, you can save time during the installation process the second time through by deselecting the checkbox, since execution of the scripts takes some time and if they have already executed, there is no need to do so again.

**Step 18** Click **Next** to proceed.

The Form Data Reporting panel appears.

**Step 19** Enter your Form Data Reporting Tables settings as described in [Form Data Reporting Tables](#). Should you decide that you need to modify some of these settings after the installation, there is a utility for you to do so. See the Modifying Form Data Reporting Configuration section of *Cisco Prime Service Catalog Reporting Guide* for more information.

**Table 7-4** Form Data Reporting Tables

Field	Definition
Dictionary table prefix	The prefix for the names of the Dictionary Tables. Default value is "DM_FDR_DICTIONARY_." It is recommended to go with this prefix.  If you must change the prefix, use only alphabetic characters and the underscore character. Do not use any numeric or special characters.
Service table prefix	The prefix for the names of the Service Tables. Default value is "DM_FDR_SERVICE_." It is recommended to go with this prefix. If you must change the prefix, use only alphabetic characters and the underscore character. Do not use any numeric or special characters.
Table columns prefix	The prefix for the field names in each table. Default value is "FIELD."  It is recommended to use the default value unless there is absolute necessity to change it. This name is used to create tables with field name like FIELD1, FIELD2, ..., FIELDn.
Text column max length	This parameter indicates the maximum size of dictionary and service table object varchar field size. The default value is 200.

**Step 20** Click **Next** to proceed. The Form Data Reporting Dictionary Settings panel appears.

**Step 21** Enter Form Data Reporting Dictionary Settings as described in [Form Data Reporting Dictionary Settings Table](#).

**Table 7-5 Form Data Reporting Dictionary Settings Table**

Field	Definition
Dictionary tables	Number of tables required in the Data Mart database to store the data for reportable dictionaries. One table is needed per reportable dictionary. The default value is 50, which is also the minimum value allowed.
Text Fields	Number of Text type fields that are used in dictionaries based on the customer form reporting analysis. The default value is 40.
Numeric fields	Number of Numeric fields that are used in dictionaries based on the customer form reporting analysis. The default value is 10.
Date fields	Number of Date fields that are used in dictionaries based on the customer form reporting analysis. The default value is 10

**Step 22** Click **Next** to proceed. The Form Data Reporting Service Settings page appears.

**Step 23** Enter your Form Data Reporting Service Settings as described in [Form Data Reporting Service Settings Table](#).

**Table 7-6 Form Data Reporting Service Settings Table**

Field	Definition
Service tables	Number of tables required in the Data Mart database to store the data for reportable dictionaries. One table is needed per reportable dictionary. The default value is 50, which is also the minimum value allowed.
Text Fields	Number of Text type fields that are used in dictionaries based on the customer form reporting analysis. The default value is 80.
Numeric fields	Number of Numeric fields that are used in dictionaries based on the customer form reporting analysis. The default value is 20.
Date fields	Number of Date fields that are used in dictionaries based on the customer form reporting analysis. The default value is 20.

**Step 24** Click **Next**. The SMTP Settings panel appears.

**Step 25** Enter your SMTP settings as described in [SMTP Settings Table](#).

**Table 7-7 SMTP Settings Table**

Field	Definition
SMTP hostname	The Hostname or IP address of the SMTP server.
SMTP port	The SMTP Port Number used by the SMTP server. Valid port numbers are from 1 to 65535. The default value is 25.
SMTP username	(Optional) The authenticated user for the SMTP server.
SMTP password	(Optional) The password for the SMTP username.
Sender email	The sender email address to be used for system generated notifications.

- Step 26** (Optional) Click the **"Test SMTP"** button to verify the connection to the SMTP server. If the test connection fails, the installer will still let you move on to the next page.
- Step 27** Click **Next** to proceed. The Pre-Installation Summary panel appears.
- The installation wizard has enough information to start the installation process. Review the settings that appear on this panel. If you need to make any changes, click Previous to go back to a particular panel and make the necessary changes. If they are correct, click Install to begin the installation of Reporting.
- The installation process may take up to 20 minutes to complete. Do not interrupt the installation wizard during this process. If the installation process completes successfully, the Install Complete panel of the installation wizard appears.
- Step 28** Click **Done** to exit the installation wizard.

## Executing create\_datasource.cmd

Perform the following steps to execute create\_datasource.cmd:

- Step 1** Open a Command Prompt window, and navigate to the `<Reporting_Install_Dir>\cognos\bin` directory.
- Step 2** Execute `create_datasource.cmd`.
- Step 3** After create\_datasource.cmd completes successfully, open a browser on the Cognos machine, and connect to the URL `http://localhost/cognos10`.
- Step 4** Enter the User ID and Password of the Service Catalog Site Administrator user, then click **OK** to log in.
- Step 5** In the UI, click the **My home** link.
- Step 6** In the top right corner of the UI, click the **Launch** link, and click the **IBM Cognos Administration** drop-down menu.
- Step 7** Click the **Configuration** tab.
- Step 8** In the left pane, click the **Data Source Connections** link.
- Step 9** In the right pane, click on "RequestCenter".
- Step 10** Skip this step if your database is SQL Server. If your database is Oracle, you must perform the steps a to f described below to modify the JDBC connection parameters.
- Click the **"Set properties - RequestCenter"** icon under the Actions column as shown below:

**Figure 7-5 Set Properties - Request Center**



- Click the Connection tab, and click the **"Edit connection string"** icon, which appears next to Connection string text box.
- Under the OCI tab, copy the value in the **"SQL\*Net connect string"** text box.

- d. Open the JDBC tab, then select the Thin radio button for Driver type, paste the connection string copied in the above step to the "Oracle Net Descriptor" text box as shown below:

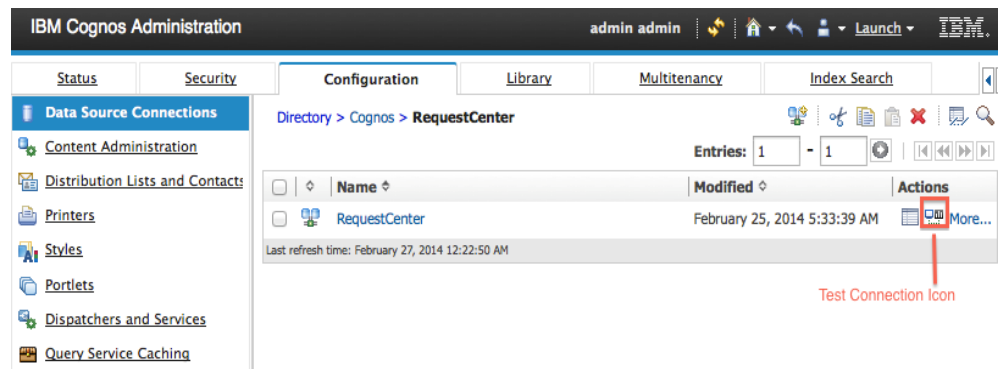
**Figure 7-6** Driver Type Selection Window



- e. Click the OK button to save the changes.  
f. Click OK button again to close the "Set properties - RequestCenter" page.

- Step 11** Perform this step for both SQL Server and Oracle. Click the "Test the connection" icon under the Actions column for RequestCenter.

**Figure 7-7** Test the Connection Window



- Step 12** On the next page, click the **Test** button.  
**Step 13** Verify that the status show "Succeeded" for both JDBC entries on the screen. You can now proceed to the next section.

## Importing Service Catalog Reports

Perform the following tasks to configure and import the Service Catalog Standard Reports Archive to the Cognos environment.

- Step 1** Open a Command Prompt window and navigate to the `<Reporting_Install_Dir>\cognos\bin` directory.  
**Step 2** Execute `import_reports.cmd`.  
**Step 3** Execute `update_datamart_std.cmd`.

**Note**

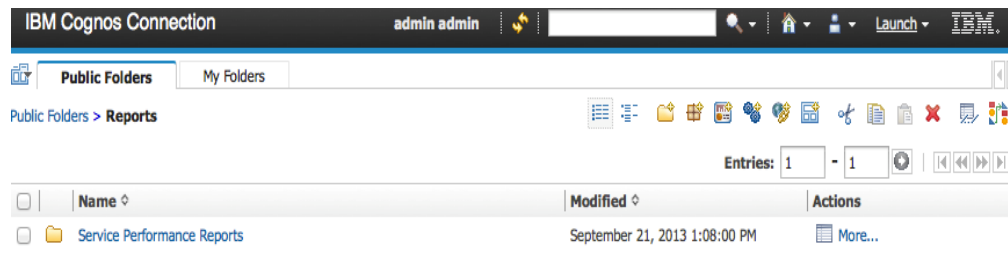
This script may take several minutes to complete.

## Restart the Service Catalog Application

Perform the following steps to restart the service catalog application:

- Step 1** **Restart the Service Catalog application.** This will allow the Service Catalog application server to pick up the new configuration which enables it to integrate with the Cognos application server. Restart the entire application server where the Request Center application is running.
- Step 2** Once the application server is started, connect to the URL using the IP address (for example, `http://IP Address/RequestCenter`). Log in as the Site Administrator user.
- Step 3** Choose the **Reporting** module.
- Step 4** Click the **Reports** tab.
- Step 5** Verify that the Public Folders tab appears with a folder named “Service Performance Reports”. This is a good indication that the Reporting module of Service Catalog is integrated successfully with the Cognos application server.

**Figure 7-8** *The Report Tab*



362597

- Step 6** Proceed to [“Configuring Advanced Reporting”](#).

## Configuring Advanced Reporting

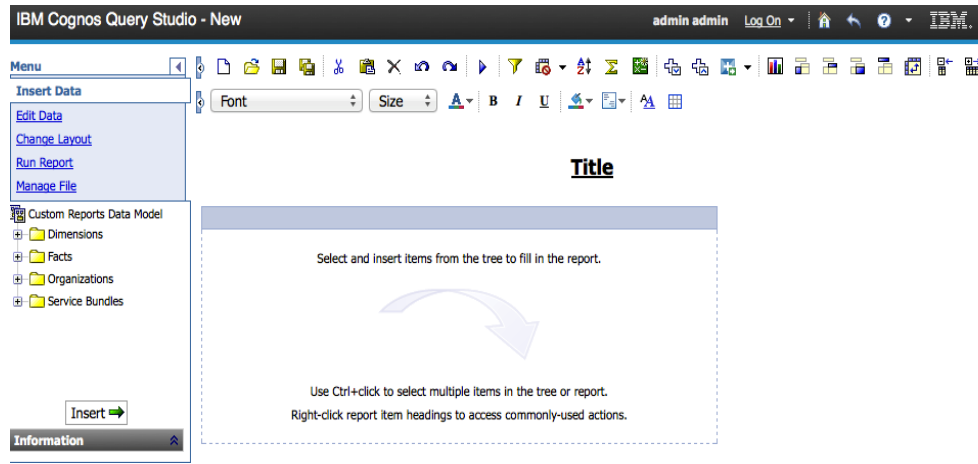
Execute the following scripts to set up the Advanced Reporting components. If you do not want Advanced Reporting, skip to the [Postinstallation Tasks](#).

- Step 1** On the Cognos machine, open a Command Prompt window, and navigate to the `<Reporting_Install_Dir>\cognos\bin` directory.
- Step 2** Execute `update_datamart.cmd`. This script may take several minutes to complete.
- Step 3** Execute `create_model.cmd`.
- Step 4** Execute `publish_fdr_pkg.cmd`. This script may take several minutes to complete.



- Step 5** Log out of the Service Catalog UI, then log back in as Site Administrator user. Remember that you must enter the ApplicationServerName on the URL which must be specified with fully qualified domain name, for example, *http://servicecatalog.mydomain.com/RequestCenter*.
- Step 6** Choose the **Advanced Reporting** module.
- Step 7** Click the **Ad-Hoc Reports** tab.
- Step 8** Click the **Custom Report Data Models** link.
- Step 9** If you see the Query Studio window, then it is a good indication that the Advanced Reporting module of Service Catalog is integrated successfully with the Cognos application server.

**Figure 7-9 Query Studio Window**



362590

## Postinstallation Tasks

The postinstallation tasks consist of scheduling the ETL processes to be run. The amount of time each process takes to complete is proportional to the amount of data in the Request Center database which must be extracted and transmitted to the Data Mart database.

## Postinstallation Tasks for Reporting

Set up the following script as scheduled tasks on the Cognos machine. All scripts reside in the `<Reporting_Install_Dir>\cognos\bin` directory.

Standard Report Script	Description
update_datamart_std.cmd	This script extracts the data from the Service Catalog database and transmits it to the Data Mart database. This data is used to refresh the Service Catalog Standard Reports. This script can be scheduled to run however often you want Standard Reports to be refreshed. Normally, this script can be scheduled to run once a day, at off-peak hours.

## Postinstallation Tasks for Advanced Reporting

If you have Advanced Reporting, then you must also perform the tasks described in this section.

- Step 1** On the Cognos machine, set up the following scripts as scheduled tasks. All scripts reside in the *<Reporting\_Install\_Dir>\cognos\bin* directory.

Advanced Report Scripts	Description
update_datamart.cmd	This script updates fact tables and dimensions in the Data Mart database.
create_model.cmd	This script creates the framework model used by the Cognos reporting tools (Query Studio and Report Studio).
publish_fdr_pkg.cmd	This script publishes the Cognos framework for Service Catalog.



**Note**

We recommend scheduling the advanced report scripts in the table above to run once daily during off-peak hours. The data in the Data Mart database are available during this time, however performance may be adversely affected.

Allow 40 minutes per 10,000 new or changed requisitions between update\_datamart.cmd and create\_model.cmd. Allow 30 minutes per 10,000 new or changed requisitions between create\_model.cmd and publish\_fdr\_pkg.cmd.

The scripts must be run without overlapping. If the scripts overlap, you may encounter data inconsistency.

## Using Reporting Module with Oracle RAC Database

When installing the Reporting module with Oracle RAC database, enter the Oracle Service Name and the IP address of the Scan Host on the installation wizard to connect to the database. After the installation, follow the steps described below to replace the Scan Host's IP address with the Scan Name. Perform these steps before you start executing the reporting configuration scripts.

- Step 1** Add the Scan Name and its set of mapped IP addresses to the machine's hosts file.
- Step 2** Stop the IBM Cognos service.
- Step 3** Replace the Scan Host's IP address with the Scan Name in all files, located in the *<Reporting Install folder>* directory and the *<Cognos Install Folder>\c10\_64* directory. The best way to do this is to use a third party software like grepWin to search which files in those directories containing the Scan Host's IP address, then use a text editor to modify those files.
- Step 4** Overwrite file ojdbc6.jar with ojdbc7.jar (which is the Oracle 12c JDBC driver) in the following directories:
- <Reporting Install folder>\cognos\lib*

<Cognos Install Folder>\c10\_64\webapps\p2pd\WEB-INF\lib

- Step 5** Replace the string "%JAVA\_HOME%\bin\java" with "%JAVA\_HOME%\bin\java -Doracle.jdbc.autoCommitSpecCompliant=false" in all scripts located in the <Reporting Install folder>\cognos\bin directory. The best way to do this is to use a third party software such as grepWin to search which files in that directory containing the string JAVA\_HOME, then use a text editor to modify those files.



**Note** Do not replace any string that looks like "%JAVA\_HOME%\bin\java.exe".

- Step 6** Use a text editor to remove the string "%DEBUG\_OPTS%" in the script "update\_datamart\_std.cmd".
- Step 7** Start the IBM Cognos service.

## Upgrading Reporting

### Performing Preupgrade Tasks for Reporting

#### Backing Up Data Mart and Content Store Artifacts

To back up the Data Mart and Content Store artifacts:

- Step 1** Back up the Data Mart database (If there are any custom Data Mart tables, they can be referred from this backup) and the Content Store database.
- Step 2** Back up all custom-defined views that are used by Advanced Reporting from the Service Catalog database.
- Step 3** Export all the backed up custom-defined views that are used by Advanced Reporting from the Service Catalog database.

#### Uninstalling Cognos 8.4.x Components

This release of Service Catalog uses Cognos version 10.2.1. You can install Cognos 10.2.1 software on a brand new machine. But if you plan to install the Cognos 10.2.1 software on the same machine where you already have Cognos 8.4.x software, then you must first uninstall the Cognos 8.4.x software, by performing the following steps:

- Step 1** From your system Start button, choose **Programs > IBM Cognos 8 > Uninstall IBM Cognos 8**.
- Step 2** Choose the display language and click **Next**.
- Step 3** Choose all the components from the package list, and proceed with the rest of the installation wizard until you get to the Finish screen.

- Step 4** Reboot the system once all the components have been uninstalled successfully.
- 

## Installing Cognos 10.2.1 Software

See [Installing Cognos Software](#) for more details on how to install Cognos 10.2.1

## Running the Reporting Installer for Upgrade

Perform the following steps to run the reporting installer for upgrade:

---

- Step 1** Run the Reporting installation wizard as described in the [Installing Reporting](#).
- Step 2** After entering values for your Data Mart Database, click **Next** to proceed to the next page of the wizard. The Existing Installation Detected dialog box appears,
- Step 3** Click **Upgrade Existing Database**.
- Step 4** Continue with the Reporting installation wizard as described in the [Running the Reporting Installation Wizard](#). You cannot edit the settings in the Form Data Reporting Tables, Form Data Reporting Dictionary Settings, and Form Data Reporting Service Settings pages. On these pages, just click **Next** to continue. Should you decide that you need to modify some of these settings after the upgrade, there is a utility for you to do so. See the Modifying Form Data Reporting Configuration section of [Cisco Prime Service Catalog Reporting Guide](#) for more information.
- 

## Performing Post-upgrade Tasks for Advanced Reporting

Perform the tasks described in [Postinstallation Tasks](#).

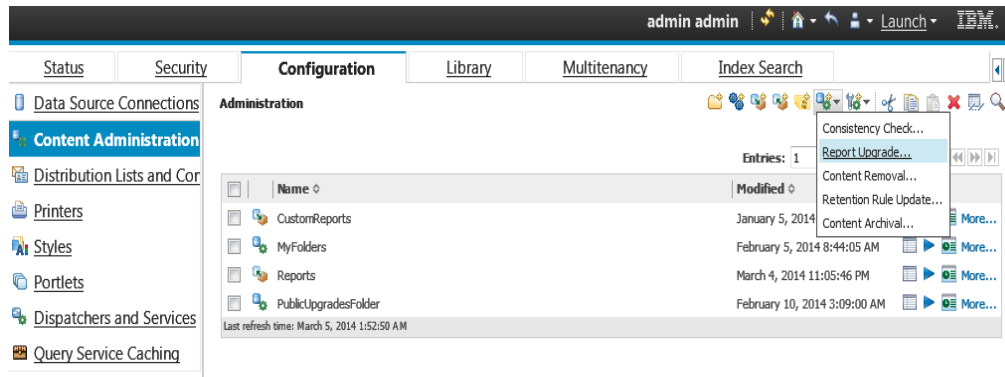
## Migrating Custom Reports

Custom reports are automatically upgraded during the Cognos upgrade to 10.1. If you wish, you could manually upgrade the reports from the Prime Service Catalog.

---

- Step 1** Log into Service Catalog as a user with the Report Administrator role.
- Step 2** Choose **Advanced Reporting** module from the drop-down.
- Step 3** Go to **Launch** on the right hand side top corner and click **IBM Cognos Administration**.
- Step 4** Click the **Configuration** tab.
- Step 5** Go to **Content Administration** from the left pane, click on the **New Content Maintenance** icon and select **Report Upgrade**, as shown below.

Figure 7-10 Content Administration Window



362596

- Step 6** Enter the Name, Description (optional) and Screen Tips (optional) for the New Content Maintenance task. And click **Next**.
- Step 7** In the Report upgrade screen, click **Add**. Select folders that need to be upgraded, click **Add**, and then at the bottom, click **OK**.
- Step 8** Click **Next**.
- Step 9** Select any of the below actions:
- Save and run once.
  - Save and schedule
  - Save only
- Step 10** Click **Finish**.
- Step 11** Select the time to run the report upgrade and click **OK**.
- Step 12** To view the result of the job select the check box “View the details of this content maintenance task after closing the dialog”.
- Step 13** Click **OK**.
- Step 14** Click **Refresh** to view the status. Click **Close**.

## Reporting Upgrade Issue and its Workaround

While upgrading from any earlier release to 10.1, except for 10.0 and 10.0-R2, certain roles under the Permission tab of the Reports, show up as Unavailable. This happens if the role is either deprecated or renamed in 10.1. This change does not impact the reporting functionality but might create confusion for the user. To avoid this, you could delete the affected roles and add them back if the role is renamed.

To delete and then add a role:

- Step 1** Log in to Service Catalog UI, and navigate to the **Advanced Reporting** module.
- Step 2** Navigate to your custom report under your folder name.
- Step 3** Click **More** under the **Actions** column for your custom report.
- Step 4** Click **Set properties** under **Available** actions.

- Step 5** Click on the **Permissions** tab. If any roles are displayed as Unavailable, it is because those roles were deprecated or renamed. You can either remove these roles if you no longer need them, or rename it to an appropriate role name based on the list of new roles that are available in this release.
- Step 6** To remove a role: Select the check box in front of the role that is displayed as Unavailable, then click the **Remove** link at the bottom of the table.
- Step 7** To add a new role: Click the **Add** link at the bottom of the table, click **newScale**, select one or more roles from the Available entries table, click the add arrow to move these roles to the Selected entries table, then click the **OK** button. Next, you have to set the appropriate permissions for the new roles that you just added. After you are done, click the **OK** button to close the Set properties page.
- 

These instructions for modifying roles are only applicable for a custom report. You cannot modify a standard report that came along with Prime Service Catalog.

## Uninstalling Reporting

To uninstall the reporting module you need to first uninstall the IBM Cognos software and then the Cisco Prime Service Catalog Reporting module.

### To uninstall IBM Cognos:

- Step 1** From the **Start** menu select **IBM Cognos 10-64 > Uninstall IBM Cognos**.
- Step 2** In the Uninstall Wizard window, click **Select All** to select both the modules.
- Step 3** Click **Next**.
- Step 4** In the Uninstall Wizard window, it is recommended that you select the second option to uninstall all the folders.
- Step 5** After the uninstallation is complete, in File Explorer, go to the folder where IBM Cognos is installed and manually delete the folder to clean up all Cognos files from the machine.
- 

### To uninstall Cisco Prime Service Catalog Reporting module

- Step 1** In File Explorer, navigate to the Cisco Prime Service Catalog Reporting folder and right click and select **Uninstall/Change**.
- Step 2** In the Uninstall Options window, select **Complete Uninstall**.
- Step 3** After the uninstallation is complete, if you still see Cisco Prime Service Catalog Reporting folder, delete it manually.
-



## **PART 1**

### **Appendices**







## Worksheets

### Database Information Worksheet

Complete the following database information worksheet by entering your configuration values in the value column. You will need the information in this worksheet when you run the Prime Service Catalog and Reporting installation wizards.

**Table A-1 Database Information Worksheet**

Field	Description	Value
<b>RequestCenter Database</b>		
Database Type	The type of RDBMS. Enter <b>Microsoft SQL Server</b> or <b>Oracle</b> .	
Host IP Address	IP address of the Database Server for the Service Catalog database.	
Port	The TCP/IP Port Number used by your Database Server. Valid port numbers are from 1 to 65535. For Microsoft SQL Server, the default value is 1433. For Oracle, the default value is 1521.	
Database Name ( <b>Microsoft SQL Server only</b> )	The name of the ServiceCatalog database. By default this is ServiceCatalog.	
Database SID or Database Service Name ( <b>Oracle only</b> )	The SID or Service Name of the Oracle server where the ServiceCatalog database resides. By default this is ORCL. Also, write down whether this value is an SID or a Service Name. When using Oracle RAC use the Service Name only.	
Username	The username that the Prime Service Catalog application uses to authenticate with the ServiceCatalog database at runtime. The default username is CPSCUser.	
Password	The password for the Database User.	
<b>Oracle Advanced Options only</b>		
Enable multiple tablespaces?	Check the check box to enable multiple tablespaces. Enter the names of the tablespaces below. This is unchecked by default.	
Default tablespace	If you checked “Enable multiple tablespaces?” above, enter the Default tablespace. The default is CCPDATA01.	
Directory tablespace	If you checked “Enable multiple tablespaces?” above, enter the Directory tablespace. The default is CCPDATA02.	


Table A-1 Database Information Worksheet (continued)

Field	Description	Value
Transaction tablespace	If you checked "Enable multiple tablespaces?" above, enter the Transaction tablespace. The default is CCPDATA03.	
Index tablespace	If you checked "Enable multiple tablespaces?" above, enter the Index tablespace. The default is CCPINDX.	

## WildFly Application Server Information Worksheet

Complete the following "Application Server Information Worksheet" by entering your configuration values in the "Value" column. The information in this worksheet will be needed when you run the Service Catalog or the Reporting installer.

Table A-2 Application Server Information Worksheet

Field	Description	Value
Service Catalog Host IP Address	Enter the IP address of the current machine. The installer should detect the IP address of the current machine automatically, and display that value as the default value.	
Service Link Host IP Address	The IP address of the computer where you plan to execute the installer, and choose to install the Service Link application.  If you choose to install both Service Catalog and Service Link applications on the same computer, the installer will automatically set this value to the same value as the "Service Catalog Host IP Address".	
IIS Website	The name of the IIS website on your computer where you want the installer to configure the tomcat plugin. The Default value is "Default Web Site".  You can use customized website. To add a customized website, you will have to add the customized website first in the Internet Information Services (IIS) Manager and bind them to appropriate port e.g. 88 ,90.	
Queue hostname	The IP address of the computer where the WildFly JMS service is running. Since the JMS service is always configured in the same WildFly server where the Service Link component resides, this value should be the same as the "Service Link Host IP Address" above.	
Custom content archive	If you plan to install "custom content", enter the path to the custom content archive file.   <b>Note</b> The archive must be in the Zip format.	
SMTP hostname	The fully qualified domain hostname or IP address of the SMTP server. Ensure that your computer can connect to this SMTP server.	
SMTP port	The SMTP server must listen to port 25.	
System email address	The sender email address to be used for system generated notifications.	

# WebLogic Application Server Information Worksheet

**Table A-3** Application Server Information Worksheet for WebLogic

Field	Description	Value
<b>Request Center Configuration</b>		
Service Catalog Host IP Address	The IP address of the computer where the WebLogic Server is running. The installer does not have to be executed on the same machine where the WebLogic server is running. So make sure that you enter the correct value for WebLogic Host IP Address here.	
Service Catalog HTTP port	The Listen Port of the WebLogic Server. Valid port numbers are from 1 to 65535. The default value is 7001.	
Service Catalog JNDI port	The JNDI Port of the WebLogic Server. This number should be set to the same value as the Listen Port of the WebLogic Server.	
Service Catalog protocol	The web protocol for the WebLogic Application Server. Choose <b>http</b> or <b>https</b> from the drop-down menu. The default is http.	
Datasource JNDI name	The datasource JNDI name for the ServiceCatalog database. This setting must have the prefix “eis/”. The default name is “eis/REQUESTCENTERDS”.	
<b>Application Server Configuration Advanced Options</b>		
Enable clustering	Check the check box to enable a Clustered Application Server environment with multiple nodes. This is unchecked by default.	
Multicast address	If you checked “Enable clustering” above, enter the multicast address.	
Custom content?	Check the check box to use Custom content. You must enter the path to the Custom content archive below.	
Custom content archive	If you checked “Custom content?” above, enter the path to the Custom content archive including the name of the archive, or click <b>Browse</b> to locate and choose the custom content archive. The archive directory structure must match the deployment directory structure. The archive must be in the Zip format.	
Install Storefront service content	Prime Service Catalog can be installed with sample Storefront content. Select this option if you want these sample content to be imported automatically into your Service Catalog database during the installation. Deselect this option if you do not want to include the sample content for your installation.  If you are upgrading from a previous Prime Service Catalog release, you should deselect this option. There is a chance that the sample Storefront content may clash with your existing data.	
<b>Service Link Configuration (Note: These settings will only be prompted if you choose the “Custom” installation option.)</b>		
Service Link hostname	The IP address of the computer where the “Service Link WebLogic Server” is running. For a standalone environment, this value is the same as the Service Catalog Host IP Address for the Application Server.	

Table A-3 Application Server Information Worksheet for WebLogic (continued)

Field	Description	Value
Service Link HTTP port	The Listen Port of the "Service Link WebLogic Server". If you have a clustered environment, then Service Link must be deployed on a separate WebLogic server outside of the cluster. Enter the port number for this separate WebLogic server. The default value is 7001.	
Service Link JNDI port	The JNDI Port of the "Service Link WebLogic Server". This number should be set to the same value as the Listen Port of the "Service Link WebLogic Server".	
Service Link protocol	The web protocol for the Service Link WebLogic Server. Choose <b>http</b> or <b>https</b> from the drop-down menu. The default is http.	
Datasource JNDI name	The datasource JNDI name for the ServiceCatalog database. This setting must have the prefix "eis/". The default name is "eis/REQUESTCENTERDS".	
<b>Messaging Configuration (Note: These settings will only be prompted if you choose the "Custom" installation option.)</b>		
Queue Host IP Address	The IP address of the computer where the JMS service is running.	
Queue port	Port Number used by your JMS service. Valid port numbers are from 1 to 65535. The default value is 7001.	
Queue username	The username of the JMS Queue User. This field is mandatory.	
Queue password	The password for the JMS Queue User. This field is mandatory.	
Queue Connection factory	The name of the JMS Queue Connection Factory. The default name is NSConnectionFactory	
<b>Messaging Queues Configuration</b>		
Authorizations queue	The name of the Authorizations Queue. The default is BEEEAuthorizationsQueue.	
Requisitions queue	The name of the Requisitions Queue. The default is BEEERequisitionsQueue.	
Service Catalog inbound queue	The name of the Service Catalog Inbound Queue. The default is BEEEinboundQueue	
Service Link inbound queue	The name of the Service Link Inbound Queue. The default is ISEEinboundQueue.	
Service Link outbound queue	The name of the Service Link Outbound Queue. The default is ISEEOutboundQueue.	
<b>Prime Service Catalog Administration Configuration</b>		
SMTP hostname	The Hostname or IP address of the SMTP server.	
SMTP port	The SMTP Port Number used by the SMTP server. Valid port numbers are from 1 to 65535. The default value is 25.	
System email address	The sender email address to be used for system generated notifications.	
Prime Service Catalog Site Administrator: Password	Password of the Cisco Prime Service Catalog site administrator, required only for a new installation.	
Prime Service Catalog Site Administrator Confirm password	Re-enter your site administrator's password to confirm.	

# Supported Time Zone

The Cisco Prime Service Catalog Reporting installer automatically sets the time zone of the Cognos server to match the time zone of the Service Catalog application. The following table shows the supported time zones for the Service Catalog application. The installer will automatically map the Service Catalog time zone to an equivalent Cognos time zone that has the same GMT offset.

Time Zone Name	Computer Time Zone Description (GMT)
Etc/GMT+12	(GMT-12:00) International Date Line West
Pacific/Apia	(GMT-11:00) Samoa
US/Hawaii	(GMT-10:00) Hawaii
US/Aleutian	(GMT-10:00) Hawaii Aleutian Daylight Time
US/Alaska	(GMT-09:00) Alaska
America/Tijuana	(GMT-08:00) Pacific Time (US and Canada); Tijuana
America/Chihuahua	(GMT-07:00) Chihuahua, La Paz, Mazatlan
US/Arizona	(GMT-07:00) Arizona
Canada/Mountain	(GMT-07:00) Mountain Time (US and Canada)
Canada/Saskatchewan	(GMT-06:00) Saskatchewan
US/Central	(GMT-06:00) Central America
Canada/Central	(GMT-06:00) Central Time (US and Canada)
America/Mexico_City	(GMT-06:00) Guadalajara, Mexico City, Monterrey
America/Bogota	(GMT-05:00) Bogota, Lima, Quito
Canada/Eastern	(GMT-05:00) Eastern Daylight Time (US and Canada)
America/Jamaica	(GMT-05:00) Eastern Time (US and Canada)
US/East-Indiana	(GMT-05:00) Indiana (East)
America/Antigua	(GMT-04:00) Atlantic Time (Canada)
Canada/Atlantic	(GMT-04:00) Atlantic Daylight Time (Canada)
America/Manaus	(GMT-04:00) Manaus
America/Santiago	(GMT-04:00) Santiago
America/Caracas	(GMT-04:30) Caracas
America/La_Paz	(GMT-04:00) La Paz (Bolivia)
America/Sao_Paulo	(GMT-03:00) Brasilia
America/Godthab	(GMT-03:00) Greenland
America/Argentina/Buenos_Aires	(GMT-03:00) Buenos Aires
America/Guyana	(GMT-04:00) Georgetown
America/St_Johns	(GMT-03:30) Newfoundland and Labrador
Atlantic/South_Georgia	(GMT-02:00) Mid-Atlantic
Atlantic/Azores	(GMT-01:00) Azores
Atlantic/Cape_Verde	(GMT-01:00) Cape Verde Islands
Etc/Greenwich	(GMT) Greenwich Mean Time: Dublin, Edinburgh,
Africa/Casablanca	(GMT) Casablanca, Monrovia
Europe/Sarajevo	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
Europe/Brussels	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
Africa/Brazzaville	(GMT+01:00) West Central Africa
Europe/Amsterdam	(GMT+01:00) Amsterdam, Berlin, Bern, Rome,

Europe/Belgrade	(GMT+01:00) Belgrade, Bratislava, Budapest,
Africa/Cairo	(GMT+02:00) Cairo
Europe/Helsinki	(GMT+02:00) Helsinki, Kiev, Riga, Sofia, Tallinn,
Europe/Minsk	(GMT+02:00) Minsk
Europe/Athens	(GMT+02:00) Athens, Bucharest, Istanbul
Asia/Jerusalem	(GMT+02:00) Jerusalem
Africa/Windhoek	(GMT+02:00) Windhoek
Africa/Harare	(GMT+02:00) Harare, Pretoria
Asia/Baghdad	(GMT+03:00) Baghdad
Africa/Nairobi	(GMT+03:00) Nairobi
Europe/Moscow	(GMT+03:00) Moscow, St. Petersburg, Volgograd
Asia/Kuwait	(GMT+03:00) Kuwait, Riyadh
Asia/Tehran	(GMT+03:30) Tehran
Asia/Baku	(GMT+04:00) Baku
Asia/Muscat	(GMT+04:00) Abu Dhabi, Muscat
Asia/Yerevan	(GMT+04:00) Yerevan
Asia/Tbilisi	(GMT+04:00) Tbilisi
Asia/Kabul	(GMT+04:30) Kabul
Asia/Karachi	(GMT+05:00) Islamabad, Karachi, Tashkent
Asia/Yekaterinburg	(GMT+05:00) Ekaterinburg
Asia/Kolkata	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
Asia/Kathmandu	(GMT+05:45) Kathmandu
Asia/Dhaka	(GMT+06:00) Astana, Dhaka
Asia/Novosibirsk	(GMT+07:00) Novosibirsk
Asia/Colombo	(GMT+05:30) Sri Jayawardenepura
Asia/Rangoon	(GMT+06:30) Yangon (Rangoon)
Asia/Bangkok	(GMT+07:00) Bangkok, Hanoi, Jakarta
Asia/Krasnoyarsk	(GMT+08:00) Krasnoyarsk
Asia/Irkutsk	(GMT+09:00) Irkutsk
Asia/Kuala_Lumpur	(GMT+08:00) Kuala Lumpur, Singapore
Asia/Taipei	(GMT+08:00) Taipei
Australia/Perth	(GMT+08:00) Perth
Asia/Chongqing	(GMT+08:00) Beijing, Chongqing, Hong Kong SAR,
Asia/Seoul	(GMT+09:00) Seoul
Asia/Tokyo	(GMT+09:00) Osaka, Sapporo, Tokyo
Asia/Yakutsk	(GMT+09:00) Yakutsk
Australia/Darwin	(GMT+09:30) Darwin
Australia/Adelaide	(GMT+09:30) Adelaide
Australia/Hobart	(GMT+10:00) Hobart
Australia/Canberra	(GMT+10:00) Canberra, Melbourne, Sydney
Australia/Brisbane	(GMT+10:00) Brisbane
Asia/Vladivostok	(GMT+10:00) Vladivostok
Pacific/Guam	(GMT+10:00) Guam, Port Moresby
Pacific/Guadalcanal	(GMT+11:00) Solomon Islands, New Caledonia
Pacific/Auckland	(GMT+12:00) Auckland, Wellington

Pacific/Fiji	(GMT+12:00) Fiji Islands
Pacific/Tongatapu	(GMT+13:00) Nuku alofa

**Note**

The Europe/Moscow, Pacific/Fiji, Pacific/Apia, Asia/Yakutsk, and Asia/Vladivostok Time Zones currently do not support Daylight Saving Time. Thus, if you have to use one of these Time Zone Names, then either use one of the other Time Zone Names that has the same GMT offset, or consult with the Cisco Technical Assistance Center (TAC).

## Reference Tables for Installation Procedures

**Note**

The installation configuration options are case-sensitive, so ensure that you enter a value, such as a database name or a JMS queue name, with case sensitivity; otherwise, your installation may fail.

**Table A-4 Database Information Worksheet**

Field	Definition for Oracle	Definition for SQL Server
Host IP Address	IP address of the database server.	IP address of the database server
Port	TCP/IP Port number used by the database server. The default value is 1521.	TCP/IP Port number used by the database server. The default value is 1433.
Database name	Not Applicable	The name of the database for the Prime Service Catalog application. Enter alphanumeric characters and do not include any space characters. The default value is "ServiceCatalog".
sa Password	Not Applicable	To create the database in SQL Server, the installer must connect to SQL Server as "sa" user. Enter the password for the sa user.
Username	Database username is the login ID and the schema name for the database schema. The default value is "CPSCUser".	Database username is the login ID and the db_owner of the "ServiceCatalog" database. The default value is "CPSCUser".
Password	Password for the database username.	Password for the database username.
Confirm Password	Re-enter the password for the database username.	Re-enter the password for the database username.



Field	Definition for Oracle	Definition for SQL Server
Oracle Service Name or Oracle SID	The SID or Service Name of the Oracle server where the ServiceCatalog database resides. By default this is ORCL. Also, write down whether this value is an SID or a Service Name. When using Oracle RAC use the Service Name only.	Not Applicable
SYS Password	To create the database schema in Oracle, the installer must connect to Oracle as the “sys” user. Enter the password for “sys” user.	Not Applicable
User tablespace	Enter a tablespace name if you already have a specific Oracle tablespace name. The default tablespace name will be set to this value. If you leave this value blank, then the installer will use the default user tablespace provided by the Oracle server.	Not Applicable



Field	Definition for Oracle	Definition for SQL Server
Temp tablespace	<p>Enter a temp tablespace name if you already have a specific Oracle tablespace name. The default temp tablespace name will be set to this value.</p> <p>If you leave this value blank, then the installer will use the default temp user tablespace name provided by the Oracle server.</p>	Not Applicable
Execute database scripts?		<p>The option is enabled only if you have clicked <b>No</b> in the ServiceCatalog Database Creation panel. This option should always be selected, which tells the installer to execute the sql scripts to either create a brand new schema in the ServiceCatalog database in the case of a new installation, or to upgrade an existing schema from a previous release to the current release in the case of an upgrade installation. (Refer to <a href="#">Chapter 6, "Upgrading Prime Service Catalog"</a>: for more detailed information on upgrading database.)</p> <p>When you want to reinstall the product WAR files without overwriting the existing ServiceCatalog database, you can deselect this option. Make sure you understand its implication before deselecting this option.</p>


**Table A-5** Service Catalog Configuration Table for WildFly


Field	Definition
Service Catalog Host IP Address	Enter the IP address of the current machine. The installer should detect the IP address of the current machine automatically, and display that value as the default value.
WildFly admin username	Since the installer will install the WildFly AS software automatically for you, it presets the WildFly admin username to "adminuser". This username can be used to connect to the WildFly Admin Console should you need to perform any administration tasks for the WildFly installation. This value is grayed out so you can't overwrite it.

Field	Definition
WildFly admin password	Enter a password for the WildFly “adminuser”. Enter only alphanumeric characters with no spaces.
Confirm password	Re-enter a password for the WildFly “adminuser”.
Service Link URL	<div style="text-align: right; margin-bottom: 10px;">  <p><b>Note</b> You will see this option if you have selected to install only the Service Catalog server on your computer.</p> </div> <p>Enter the http address that includes the hostname and portnumber of Service Link server. The default port number used by Service Link on WildFly in 6080.</p>
Configure as windows service	<p>(For Windows only) On Windows Operating System, the installer can automatically configure the WildFly server as a windows service. Select this option if you would like the installer to configure the WildFly server as a service named “Cisco Prime Service Catalog”. This service will be configured to start up automatically at boot time. But right after the installation is completed, the service will not be started up for you. You will have to open the Microsoft Windows Services Console to start the “Cisco Prime Service Catalog” service for the first time after the installation. The service however will be started automatically when the Windows Operating System is rebooted.</p> <p><b>Note</b> However, for cluster WildFly it is recommended to start the server as an application, instead of service, by executing the start script provided by Cisco. For information on starting these services, see <a href="#">Postinstallation Tasks for WildFly Standalone Application Server</a> or <a href="#">Postinstallation Tasks for WildFly Clustered Application Servers</a>.</p>
Configure IIS	<p>(For Windows only) If the installer detects that IIS web server is installed on the same Windows machine where you execute the installer, it will present this option on the panel screen. Select this option if you would like the installer to automatically configure the tomcat plugin for the IIS web server to connect to the WildFly application server, which runs on the same machine.</p> <div style="text-align: right; margin-bottom: 10px;">  <p><b>Note</b> If you plan to install Cognos software (see <a href="#">Installing Cognos Software</a>) on the same Windows machine where you are installing WildFly, then you must deselect the “Configure IIS” option at this time. IIS must be used for the Cognos software when you install Cognos and the Reporting module.</p> </div> <p>If you select this option, the installer will perform validation test against the IIS web server. If it detects that the IIS web server is missing some required settings, then the validation test will fail, and the installer will not let you proceed unless you deselect the “Configure IIS” option. (Refer the Software Configuration Prerequisites section for more information on IIS requirements.)</p>

Field	Definition
IIS Web site	<p>This option is enabled only when you select the "Configure IIS" option above. Enter the name of the IIS site which already exists, that you want the installer to configure the tomcat plugin. The default value is "Default Web Site".</p> <p>You can use customized website. To add a customized website, you will have to add the customized website first in the Internet Information Services (IIS) Manager and bind them to appropriate port e.g. 88 ,90.</p>
Install Storefront service content	<p>Prime Service Catalog can be installed with sample Storefront content. Select this option if you want these sample content to be imported automatically into your ServiceCatalog database during the installation. Deselect this option if you do not want to include the sample content for your installation.</p> <p>If you are upgrading from a previous Prime Service Catalog release, you should deselect this option. There is a chance that the sample Storefront content may clash with your existing data.</p>

**Table A-6** Service Link Configuration Table for WildFly



Variable	Definition
Service Link Host IP Address	<p>This value is preset to the same value that you entered for the Service Catalog host IP address field on the Service Catalog Configuration panel. This is because both WildFly servers, one for Service Catalog application and one for Service Link application, will be running on the same machine. This value is grayed out so you can't overwrite it.</p>
WildFly admin username	<p>The installer has preset the WildFly admin username to "adminuser" because it will install the WildFly AS software automatically for you. This username can be used to connect to the WildFly Admin Console if you need to perform any administration tasks for the WildFly installation. This value is grayed out so you can't overwrite it.</p> <p> <b>Note</b> Field "WildFly admin password" is not presented on this panel. This is because the password is preset to the same value that you entered for the WildFly admin password field on the Service Catalog Configuration panel.</p>

Variable	Definition
Configure as windows service	<p>(For Windows only) On Windows Operating System, the installer can automatically configure the WildFly server as a windows service. Select this option if you would like the installer to configure the WildFly server as a service named "Cisco Prime Service Link". This service will be configured to start up automatically at boot time. But right after the installation is completed, the service will not be started up for you. You will have to open the Microsoft Windows Services Console to start the "Cisco Prime Service Link" service for the first time after the installation. The service however will be started automatically when the Windows Operating System is rebooted. For more information on starting these services, see <a href="#">Starting WildFly Server on Windows</a>.</p>
Configure IIS	<p>(For Windows only) If the installer detects that IIS web server is installed on the same Windows machine where you execute the installer, it will present this option on the panel screen.</p> <p>Select this option if you would like the installer to automatically configure the tomcat plugin for the IIS web server to connect to the WildFly application server, which runs on the same machine.</p> <p> <b>Note</b> If you plan to install Cognos software (see <a href="#">Installing Cognos Software</a>) on the same Windows machine where you are installing WildFly, then you must deselect the "Configure IIS" option at this time. IIS must be used for the Cognos software when you install Cognos and the Reporting module.</p> <p>If you select this option, the installer will perform validation test against the IIS web server. If it detects that the IIS web server is missing some required settings, then the validation test will fail, and the installer will not let you proceed unless you deselect the "Configure IIS" option. (Refer the Software Configuration Prerequisites section for more information on IIS requirements.)</p>
IIS Web Site	<p>This option is enabled only when you select the "Configure IIS" option above. Enter the name of the IIS site which already exists, that you want the installer to configure the tomcat plugin. The default value is "Default Web Site".</p> <p>You can use customized website. To add a customized website, you will have to add the customized website first in the Internet Information Services (IIS) Manager and bind them to appropriate port e.g. 88 ,90.</p>

**Table A-7 Messaging Configuration Table**

<b>Field</b>	<b>WildFly</b>	
Queue Host IP Address	Enter the IP address of the machine where Service Link is installed, because JMS service resides on the Service Link node.	
Queue Port	Port number for communicating to the Service Link node.	
Queue connection factory	Value of JMS Queue Connection Factory for WildFly is preset to "jms/RemoteConnectionFactory", and is grayed out.	Default value of JMS Queue Connection Factory for WebLogic is "NSConnectionFactory"
Queue username	Username that can have read/write access to JMS Queues. This Value for WildFly is preset to "jmsuser", and is grayed out.	The value of username for WebLogic is "weblogic".
Queue password	For WildFly, enter a password for the "jmsuser". The "jmsuser" will be created by the installer when it installs the WildFly software.	Enter the password for the "weblogic" user.
Confirm password	This field is applicable for WildFly only. Re-enter the password for the "jmsuser".	Not Applicable

**Table A-8 Service Catalog Administration Configuration Table**

Field	Definition
SMTP hostname	<p>Enter the fully qualified domain hostname or IP address of the SMTP server. The Service Catalog application will connect to this SMTP server to send out all email notifications.</p> <p> <b>Note</b> There is an optional Test SMTP button on this panel. After you enter the SMTP hostname and system email address, you can click the Test SMTP button to verify the connection to the SMTP server. The installer will display a message dialog which shows whether the Test connection to the SMTP server succeeds or fails. If the SMTP server test connection fails, the installer will still let you move on to the next step. Just close the message dialog, then Click Next to continue.</p>
SMTP Port	The SMTP server must be listening to port 25.
System email address	Enter the email address of the system administrator. This is used as the sender's email address for all system-level email notifications.
Service Catalog Site Administrator Password	<p>(This option is not shown for an "upgrade" installation.)</p> <p>Enter the password for the Site Administrator of the application. The password cannot be blank. Enter alphanumeric characters for the password.</p> <p> <b>Note</b> The Site Administrator's username is preset to "admin" and can not be changed.</p>
Confirm Password	<p>(This option is not shown for an "upgrade" installation.)</p> <p>Re-enter the password for Site Administrator.</p>

**Table A-9 Service Catalog Configuration for WebLogic**

Field	WebLogic
Service Catalog hostname	<p>Enter the fully qualified domain hostname or IP address of the machine where the WebLogic server is running.</p> <p>The installer does not have to be executed on the same machine where the WebLogic server is running. So make sure that you enter the correct value for WebLogic hostname here.</p>
Service Catalog HTTP port	Enter the Listen Port number assigned to the WebLogic server. The default value is 7001.
Service Catalog JNDI port	Enter the Listen Port number assigned to the WebLogic server. The default value is 7001.

Field	WebLogic
Service Catalog protocol	Select the value "http" from the drop-down list. If you select "https", then your WebLogic server must already be SSL-enabled. In this case, make sure you enter the value of the SSL Listen Port for your WebLogic server in the "Service Catalog HTTP port" field above.
Datasource JNDI name	Enter the datasource JNDI name for the Service Catalog database which you have already configured for the WebLogic server as a prerequisite. The default value is "eis/REQUESTCENTERDS".
Data Mart JNDI name	Enter the datasource JNDI name for the Data Mart database here. The Data Mart database is needed if you plan to install the Reporting module. If you don't have the Reporting module, you can leave this value blank. The default value is "eis/DATAMARTDS".
Install Storefront service content	<p>Prime Service Catalog can be installed with sample Storefront content. Select this option if you want these sample content to be imported automatically into your ServiceCatalog database during the installation. Deselect this option if you do not want to include the sample content for your installation.</p> <p>If you are upgrading from a previous Prime Service Catalog release, you should deselect this option. There is a chance that the sample Storefront content may clash with your existing data.</p>

**Table A-10 Database Information Table for Advanced Installation**

Field	Definition for SQL Server	Definition for Oracle
Hostname	Hostname or IP address of the database server	Hostname or IP address of the database server
Port	TCP/IP Port number used by the database server. The default value is 1433.	TCP/IP Port number used by the database server. The default value is 1521.
Oracle Service Name or Oracle SID	Not Applicable	If you use Service Name to connect to your Oracle database, then select the Service Name radio button, and enter the Service Name value. If you use SID to connect to your Oracle database, then select the SID radio button, and enter the Oracle SID value.
Username	Database username is the login ID and the db_owner of the "ServiceCatalog" database. The default value is "CPSCUser".	Database username is the login ID and the schema name for the database schema. The default value is "CPSCUser".
Password	Password for the database username.	Password for the database username.

Field	Definition for SQL Server	Definition for Oracle
Execute Database Scripts?		<p>The option is enabled only if you have clicked <b>No</b> in the ServiceCatalog Database Creation panel. This option should always be selected, which tells the installer to execute the sql scripts to either create a brand new schema in the ServiceCatalog database in the case of a new installation, or to upgrade an existing schema from a previous release to the current release in the case of an upgrade installation. (Refer to <a href="#">Chapter 6, “Upgrading Prime Service Catalog”</a> for more detailed information on upgrading database.)</p> <p>When you want to reinstall the product WAR files without overwriting the existing ServiceCatalog database, you can deselect this option. Make sure you understand its implication before deselecting this option.</p>
Advanced Options (for Oracle only)		This button is available in the ServiceCatalog Database window for Oracle only. When you click this button, Advanced Options window with the following files is displayed. Click <b>Close</b> after you enter the required details in the Advanced Options window.
Enable multiple tablespace? (for Oracle only)		Select this option if your existing ServiceCatalog database was created on multiple table spaces on Oracle.
Default tablespace (for Oracle only)		The name of the tablespace where all of the definitional-data tables are created. Definitional-data tables have names that start with DEF. The default value is CCPDATA01
Directory tablespace (for Oracle only)		The name of the tablespace where all of the directory-data tables are created. Directory-data tables have names that start with DIR. The default value is CCPDATA02
Transaction tablespace (for Oracle only)		<p>The name of the tablespace where all of the transactional-data tables are created. Transactional-data tables have names that start with TX. The default value is CCPDATA03.</p> <p>Any tables whose names are different from DEF, DIR or TX are stored in the Default tablespace</p>
Index tablespace (for Oracle only)		The name of the tablespace where all of the table indexes are created. The default value is CCPINDX.

**Table A-11**      **Advanced Options Table for Service Catalog Configuration panel**



Field	Definition
Enable clustering	This option is not available for WildFly and is grayed out. For WebLogic, select this option if you have a Clustered WebLogic environment.
Multicast address	This option is not available for WildFly and is grayed out. For WebLogic, if you select the Enable clustering option above, then you must enter a multicast IP address, which the Service Catalog application uses to communicate among the different nodes in the Cluster.
Custom content?	Select this option if you want to insert custom contents into the RequestCenter.war during the installation. After the installation your deployed RequestCenter.war directory will contain the custom contents, such as ISF and custom stylesheets. This is an optional step. If you don't install Custom Content at installation time, then after the installation, you can always extract the Content zip file manually on top of the deployed RequestCenter.war directory.
Custom content archive	Enter the location of the zip file that contains the custom contents. The zip file must adhere to the directory structure underneath RequestCenter.war directory. For example, inside the content.zip file, there are the following contents: <ul style="list-style-type: none"> <li>• isfcode\*</li> <li>• custom\mystyle\*</li> <li>• images\*</li> </ul> Everything will be extracted under the RequestCenter.war stage directory, keeping the same directory structure intact.

**Table A-12** Service Link Configuration Table for Custom Installation using WildFly Server

Variable	Definition
Service Link Hostname	This value is preset to the same value that you entered for the Service Catalog hostname field on the Service Catalog Configuration panel. This is because both WildFly servers, one for Service Catalog application and one for Service Link application, will be running on the same machine. This value is grayed out so you cannot overwrite it.
WildFly admin username	The installer has preset the WildFly admin username to "adminuser" because it will install the WildFly AS software automatically for you. This username can be used to connect to the WildFly Admin Console if you need to perform any administration tasks for the WildFly installation. This value is grayed out so you can't overwrite it.


Variable	Definition
WildFly admin password	<p>If you chose to install only Service Link server on this computer, then the installer will prompt you to enter the password for the WildFly administrator user.</p> <p>This field will not be shown if you chose the "Both" option instead. This is because the password is preset to the same value that you entered for the WildFly admin password field on the Service Catalog Configuration panel.</p>
Confirm password	<p>Re-enter the password for the WildFly administrative user.</p> <p>This field will not be shown if you chose the "Both" option.</p>
Configure as windows service	<p>(For Windows only) On Windows Operating System, the installer can automatically configure the WildFly server as a windows service. Select this option if you would like the installer to configure the WildFly server as a service named "Cisco Prime Service Link".</p> <p>This service will be configured to start up automatically at boot time. But right after the installation is completed, the service will not be started up for you. You will have to open the Microsoft Windows Services Console to start the "Cisco Prime Service Link" service for the first time after the installation. The service however will be started automatically when the Windows Operating System is rebooted.</p>

**Table A-13** *Messaging Configuration Table for Custom Installation*

Field	Definition for WildFly	Definition for WebLogic
Queue hostname	<p>Enter the fully qualified domain hostname or IP address of the JMS server.</p> <p>The JMS server is same as the Service Catalog server.</p>	<p>The JMS server can reside in any WebLogic server. But if you deploy Service Catalog in a Clustered WebLogic, then the JMS server needs to be configured on the WebLogic server where you deploy Service Link.</p>
Queue port	<p>Enter the JNDI Port assigned to the Service Catalog server. The default value is 4447.</p>	<p>Enter the Listen Port number assigned to the WebLogic server. The default value is 7001.</p>
Queue connection factory	<p>For WildFly, this value is preset to "jms/RemoteConnectionFactory", and thus is grayed out</p>	<p>The default value is "NSConnectionFactory"</p>
Queue Username	<p>Username that can have read/write access to JMS Queues. This Value for WildFly is preset to "jmsuser", and is grayed out.</p>	<p>The value of username for WebLogic is "weblogic".</p>

Field	Definition for WildFly	Definition for WebLogic
Queue password	For WildFly, enter a password for the "jmsuser". The "jmsuser" will be created by the installer when it installs the WildFly software.	Enter the password for the "weblogic" user.
Confirm Password	This field is applicable for WildFly only. Re-enter the password for the "jmsuser".	Not Applicable

**Table A-14 Service Link Configuration Table for Custom Installation using WebLogic**

Field	Definition for WebLogic
Service Link hostname	<p>Enter the fully qualified domain hostname or IP address of the machine where the WebLogic server is running.</p> <p> <b>Note</b> The installer does not have to be executed on the same machine where the WebLogic server is running. So make sure that you enter the correct value for WebLogic hostname here.</p>
Service Link HTTP Port	Enter the Listen Port number assigned to the WebLogic server. The default value is 7001.
Service Link JNDI port	Enter the Listen Port number assigned to the WebLogic server. The default value is 7001
Service Link protocol	Select the value "http" from the drop down list. If you select "https", then your "Service Link WebLogic Server" must already be SSL-enabled. In this case, make sure you enter the value of the SSL Listen Port for your "Service Link WebLogic Server" in the "Service Link HTTP port" field above.
Datasource JNDI name	Enter the datasource JNDI name for the ServiceCatalog database which you have already configured for the WebLogic server as a prerequisite. The default value is "eis/REQUESTCENTERDS".





## WildFly Scripts

### Scripts for WildFly Standalone Application Server

Standalone WildFly deployment includes a ServiceCatalogServer and ServiceLinkServer that can be installed on the same application server or on different servers.

Following are the start and stop scripts available in the installer for Standalone WildFly deployments.

**Table B-1** *Scripts for WildFly Standalone Application Server*

Scripts	Execute On	Description
startServiceCatalog	VM1	Start Service Catalog on VM1
startServiceLink	VM1	Start Service Link on VM1
stopServiceCatalog	VM1	Stop Service Catalog on VM1
stopServiceLink	VM1	Stop Service Link on VM1

### Scripts for WildFly Cluster Application Server

Cluster setup for WildFly can be configured in two VM or four VM topology.

**Two VM topology:**

- VM 1 is Domain Controller, Host Controller, and Service Link for Host 1
- VM 2 is Host Controller for Host 2

**Four VM topology:**

- VM 1 is Domain Controller
- VM 2 is standalone Service Link
- VM 3 is Host Controller for Host 1
- VM 4 is Host Controller for Host 2

Table B-2 Scripts for WildFly Cluster Application Server


Scripts	Execute On	Description
<b>2 VM Cluster Topology:</b>		
<b>VM1 is Domain Controller, HC1, and Service Link and VM2 is HC2.</b>		
startServiceCatalogCluster	VM1	Start the following servers on VM1: a) Domain Controller, b) Process Controller, c) Managed server for Service Link, d) Managed server for Service Catalog.   <b>Note</b> startServiceCatalogCluster script is used to check whether the exploded \$JBOSS_HOME/content/RequestCenter.war and \$JBOSS_HOME/content/ISEE.war are already available. If yes, then the script will not create the content folder. If not, then it will explode the WAR files from /dist folder and create the content folder under these directories. This is applicable for VM1 and VM2 in two VM topology and for VM 3 and VM 4 in four VM topology.
startServiceCatalogOnHC1	VM1	Start the Managed server for Service Catalog on VM1
startServiceLinkOnHC1	VM1	Start the Managed server for Service Link on VM1.
startServiceCatalogOnHC2	VM1	Start the Managed server for Service Catalog on VM2.
startServiceCatalogOnHC3	VM1	Start the Managed server for Service Catalog on VM3. (Reserved for when user wants to add Host Controller 3.)
startServiceCatalogOnHC4	VM1	Start the Managed server for Service Catalog on VM3. (Reserved for when user wants to add Host Controller 4.)
deployServiceCatalogCluster all	VM1	Deploy the followings: a) ISEE.war, b) RequestCenter.war
deployServiceCatalogCluster RC	VM1	Deploy RequestCenter.war
deployServiceCatalogCluster SL	VM1	Deploy ISEE.war
shutdownAllOnHC1	VM1	Stop the following servers on VM1: a) Domain Controller, b) Process Controller, c) Managed server for Service Link, d) Managed server for Service Catalog.
forceStopAllOnHC	VM1	If for some reasons, the shutDownAllOnHC1 script doesn't work, then execute this script to force stop the following servers on VM1: a) Domain Controller, b) Process Controller, c) Managed server for Service Link, d) Managed server for Service Catalog
stopServiceCatalogOnHC1	VM1	Stop the Managed server for Service Catalog on VM1.
stopServiceLinkOnHC1	VM1	Stop the Managed server for Service Link on VM1.
stopServiceCatalogOnHC2	VM1	Stop the Managed server for Service Catalog on VM2.
shutdownAllOnHC2	VM1	Stop both the Process Controller and the Managed server on VM2.

Table B-2 Scripts (continued) for WildFly Cluster Application Server

Scripts	Execute On	Description
stopServiceCatalogOnHC3	VM1	Stop the Managed server for Service Catalog on VM3. (Reserved for when user wants to add HC3.)
shutdownAllOnHC3	VM1	Stop both the Process Controller and the Managed server on VM3. (Reserved for when user wants to add HC3.)
stopServiceCatalogOnHC4	VM1	Stop the Managed server for Service Catalog on VM3. (Reserved for when user wants to add HC4.)
shutdownAllOnHC4	VM1	Stop both the Process Controller and the Managed server on VM4. (Reserved for when user wants to add HC4.)
undeployServiceCatalogCluster all	VM1	Undeploy the followings: a) ISEE.war, b) RequestCenter.war
undeployServiceCatalogCluster RC	VM1	Undeploy RequestCenter.war
undeployServiceCatalogCluster SL	VM1	Undeploy ISEE.war
startServiceCatalogCluster	VM2	Start the following servers: a) Process Controller, b) Managed server for Service Catalog.  The script is used to check whether the exploded \$JBOSS_HOME/content/RequestCenter.war and \$JBOSS_HOME/content/ISEE.war are already available. If yes, then the script will not create the content folder. If not, then it will explode the WAR files from /dist folder and create the content folder under these directories.
forceStopAllOnHC	VM2	Force stop: a) Process Controller, b) Managed server for Service Catalog.
<b>If customer adds another VM as HC3</b>		
startServiceCatalogCluster	VM3	Start the following servers: a) Process Controller, b) Managed server for Service Catalog.
forceStopAllOnHC	VM3	Force stop: a) Process Controller, b) Managed server for Service Catalog.
<b>If customer adds another VM as HC4</b>		
startServiceCatalogCluster	VM4	Start the following servers: a) Process Controller, b) Managed server for Service Catalog.
forceStopAllOnHC	VM4	Force stop: a) Process Controller, b) Managed server for Service Catalog.
<b>4 VM Cluster Topology:</b>		
<b>VM1 is Domain Controller, VM2 is Standalone for Service Link, VM3 is HC1, VM4 is HC2</b>		
startServiceCatalogCluster	VM1	Start the Domain Controller on VM1.
startServiceCatalogOnHC1	VM1	Start the Managed server for Service Catalog on VM3.
startServiceCatalogOnHC2	VM1	Start the Managed server for Service Catalog on VM4.

Table B-2 Scripts (continued) for WildFly Cluster Application Server

Scripts	Execute On	Description
startServiceCatalogOnHC3	VM1	Start the Managed server for Service Catalog on VM5. (Reserved for when user wants to add HC3.)
startServiceCatalogOnHC4	VM1	Start the Managed server for Service Catalog on VM6. (Reserved for when user wants to add HC4.)
deployServiceCatalogCluster RC	VM1	Deploy RequestCenter.war
stopDomainController	VM1	Stop the Domain Controller on VM1.
stopServiceCatalogOnHC1	VM1	Stop the Managed server for Service Catalog on VM3.
shutdownAllOnHC1	VM1	Stop both the Process Controller and the Managed server on VM3.
stopServiceCatalogOnHC2	VM1	Stop the Managed server for Service Catalog on VM4.
shutdownAllOnHC2	VM1	Stop both the Process Controller and the Managed server on VM4.
stopServiceCatalogOnHC3	VM1	Stop the Managed server for Service Catalog on VM5. (Reserved for when user wants to add HC3.)
shutdownAllOnHC3	VM1	Stop both the Process Controller and the Managed server on VM5. (Reserved for when user wants to add HC3.)
stopServiceCatalogOnHC4	VM1	Stop the Managed server for Service Catalog on VM6. (Reserved for when user wants to add HC4.)
shutdownAllOnHC4	VM1	Stop both the Process Controller and the Managed server on VM6. (Reserved for when user wants to add HC4.)
undeployServiceCatalogCluster RC	VM1	Undeploy RequestCenter.war
<b>VM1 is Domain Controller, VM2 is Standalone for Service Link, VM3 is HC1, and VM4 is HC2</b>		
StartServiceLink	VM2	Start Service Link on VM2.
StopServiceLink	VM2	Stop Service Link on VM2.
<b>VM1 is Domain Controller, VM2 is Standalone for Service Link, VM3 is HC1, and VM4 is HC2</b>		
startServiceCatalogCluster	VM4	Start the following servers: a) Process Controller, b) Managed server for Service Catalog.  The script is used to check whether the exploded \$JBOSS_HOME/content/RequestCenter.war and \$JBOSS_HOME/content/ISEE.war are already available. If yes, then the script will not create the content folder. If not, then it will explode the WAR files from /dist folder and create the content folder under these directories.
forceStopAllOnHC	VM4	Force stop: a) Process Controller, b) Managed server for Service Catalog.
<b>If customer adds another VM as HC3</b>		
startServiceCatalogCluster	VM5	Start the following servers: a) Process Controller, b) Managed server for Service Catalog.
forceStopAllOnHC	VM5	Force stop: a) Process Controller, b) Managed server for Service Catalog.
<b>If customer adds another VM as HC4</b>		



Table B-2 Scripts (continued) for WildFly Cluster Application Server

Scripts	Execute On	Description
startServiceCatalogCluster	VM6	Start the following servers: a) Process Controller, b) Managed server for Service Catalog.
forceStopAllOnHC	VM6	Force stop: a) Process Controller, b) Managed server for Service Catalog.

## Adding Subsequent Host Nodes Manually in WildFly Cluster

### Before You Begin

1. Run the GUI Installer for the host controller setup on the subsequent node, vm<N>, where N is the number of the node.
2. Select the Host Controller in the Node Type Selection panel followed by Host1 as the cluster node.
3. Do not run any of the startup-scripts.

**Step 1** Rename host1.xml to host<N>.xml. The file, host1.xml is present under the *InstallationDirectory/wildfly-10.1.0.Final/domain/configuration* directory.

**Step 2** Follow the below steps to create a new user:

- a. Execute **add-user.sh** or **add-user.bat** script from *InstallationDirectory/wildfly-10.1.0.Final/bin* location.
- b. Enter a to select the Management User.
- c. Provide **HOST<N>** as the Username.
- d. Provide **HOST<N>** as the Password.
- e. Enter yes to use the entered password.
- f. Re-Enter **HOST<N>** for Password confirmation.
- g. Press **Enter** to pass the management group information
- h. Enter **yes** to add the user 'HOST<N>' for realm 'ManagementRealm'.
- i. Enter **no** for the interconnection of AS process.



### Note

- The new user needs to be created in the machine having host Controller(host<N>) and domain controller (host1) as well.
- Verify that the user is added in the *InstallationDirectory/wildfly-10.1.0.Final/domain/configuration/mgmt-users.properties*

**Step 3** Perform the following changes in host<N>.xml:

- a. Change the name of Host from HOST1 to HOST<N>.location for host<N>.xml. This file is available in the C:\Installation\_directory\wildfly-10.1.0.Final\domain\configuration
 

```
<host name="HOST5" xmlns="urn:jboss:domain:2.2">
```

- b. Change the secret value in the <server-identities> section. The secret value can be obtained from the website [www.motobit.com](http://www.motobit.com):

```
<secret value="SE9TVDU="/>
```

Enter the URL <http://www.motobit.com/util/base64-decoder-encoder.asp>

- Enter HOST<N> in the text box (without any extra space or newline).
- Click on Convert the Source Data button.

- c. Change the name of the server instance from server-host1-RC to server-host<N>-RC to avoid name conflicts:

```
<server name="server-host<N>-RC" group="main-server-group" auto-start="true">
```

- d. Change the CONTROLLER\_TYPE from host1 to host<N> in setEnv.cmd script in *InstallationDirectory/bin* directory.
- e. Delete the logs and servers directories from *InstallationDirectory/wildfly-10.1.0.Final/domain*, if exists.

**Step 4** The following changes need to be done in startServiceCatalogCluster.cmd script in *InstallationDirectory/bin* directory.

- a. Add the following code snippet in BOLD in the script file:

```
#Below if condition is applicable for the windows OS platform

if "%CONTROLLER_TYPE%"=="host<N>" (
    if exist "%WILDFLY_BASE_DIR%\configuration\domain.xml" rename
"%WILDFLY_BASE_DIR%\configuration\domain.xml" "domain_backup.xml"
)

#Below if condition is applicable for the Linux OS platform

#pause 'Press [Enter] key to continue6...'
FILE=${WILDFLY_BASE_DIR}/configuration/host<N>.xml
if [ "${CONTROLLER_TYPE}" == "host<N>" ]
then
    if [ -f "$FILE" ]
    then
        /bin/mv -i ${WILDFLY_BASE_DIR}/configuration/host<N>.xml
${WILDFLY_BASE_DIR}/configuration/host.xml
    fi
fi
```

- b. Add the following code snippet in BOLD in the script file:

```
if "%CONTROLLER_TYPE%"=="host<N>" if exist "%WILDFLY_BASE_DIR%\configuration\host<N>.xml"
rename "%WILDFLY_BASE_DIR%\configuration\host<N>.xml" "host.xml"
```

If the Platform is Linux OS , skip the step b and proceed. above if condition only applicable for the windows OS platform.

- Step 5** Start the server with startServiceCatalogCluster.cmd or sh and once it is up, verify from the Wildfly admin server console under the domain whether the host<N> is registered.
- Step 6** Addition of scripts for both 4-VM Cluster and 2-VM Cluster in the VM-1 machine (machine containing the domain controller)
- a. Copy *shutdownAllOnHCL.cmd* and rename the copied script as *shutdownAllOnHC<N>.cmd*

- b. Copy `startServiceCatalogOnHC1.cmd` and rename the copied script as `startServiceCatalogOnHC<N>.cmd`
- c. Copy `stopServiceCatalogOnHC1.cmd` and rename the copied script as `stopServiceCatalogOnHC<N>.cmd`

**Note**

In the Linux platform if new scripts does not have the read/write permission, you should manually assign the read/write permission before executing.

- d. Perform the below operations in the `stopServiceCatalogOnHC<N>.cmd` script file cautiously:
  - Rename HOST1 to HOST<N>.
  - Rename host1 to host<N>.

## Configuring Plugin for IIS Web Server

This section provides information on how to configure the plugin for IIS web server (version 8.x) on a Windows Server 2012 R2 machine to redirect to clustered Wildfly application servers (version 10.1.0.Final).

To configure plugin got IIS Web Server:

- Step 1** [Add Web Server Role for IIS.](#)
- Step 2** [Install Tomcat Plugin.](#)
- Step 3** [Copy WAR Directories.](#)
- Step 4** [Create Virtual Directories for IIS.](#)
- Step 5** [Modify Plugin Properties.](#)
- Step 6** [Configure Instance-ID for WildFly.](#)
- Step 7** [Test IIS.](#)

## Add Web Server Role for IIS

- Step 1** Navigate to **Service Manager Dashboard > Manage Tab > Add Roles and Features.**
- Step 2** Add the role **Web Server (IIS)** on your Windows Server 2012 R2 operating system. Make sure you select the **ISAPI Extensions** and **ISAPI Filters** role services when adding IIS.
- Step 3** After adding the **Web Server (IIS) Role**, start the **World Wide Web Publishing Service.**
- Step 4** Launch a browser and connect to **URL = http://localhost.** You should see the **Welcome IIS 8.x** page.

## Install Tomcat Plugin

- 
- Step 1** Download the **PSC 11.x** software package from cisco.com and extract it.
  - Step 2** Cd to `<PSC_Software_Extract_Dir>\isapi` directory.
  - Step 3** Copy file **tomcat-isapi-redirector-v1.2.37.zip** to your IIS web server machine and extract it under the `C:\inetpub\isapi` directory.




---

**Note** Create the *isapi* sub-directory under `C:\inetpub` first if necessary.

---

- Step 4** Cd to `C:\inetpub\isapi` and rename the file **isapi\_redirect-1.2.37-win64.dll** to **isapi\_redirect.dll**.

## Copy WAR Directories

If you have WildFly installation and your IIS is on a separate machine from WildFly, then perform the following steps to copy WAR directories:

### Standalone WildFly Installation

- 
- Step 1** On the WildFly machine where the **RequestCenter Server** is running, **cd** to the `<PSC_Install_Dir>\wildfly-10.1.0.Final\ServiceCatalogServer\deployments` directory.
  - Step 2** Copy the entire **RequestCenter.war** sub-directory from this machine to the IIS machine and place it under the `C:\inetpub\WAR\` directory.
  - Step 3** On the WildFly machine where the **ServiceLink server** is running, **cd** to the `<PSC_Install_Dir>\wildfly-10.1.0.Final\ServiceLinkServer\deployments` directory.
  - Step 4** Copy the entire **ServiceLink.war** sub-directory from this machine to the IIS machine and place it under the `C:\inetpub\WAR\` directory.

### Clustered WildFly installation with Four VM Topology

- 
- Step 1** On the WildFly machine where one of the cluster nodes for **RequestCenter** is running, **cd** to the `<PSC_Install_Dir>\wildfly-10.1.0.Final\content` directory.
  - Step 2** Copy the entire **RequestCenter.war** sub-directory from this machine to the IIS machine and place it under the `C:\inetpub\WAR\` directory.
  - Step 3** On the WildFly machine where the **ServiceLink server** is running, **cd** to the `<PSC_Install_Dir>\wildfly-10.1.0.Final\ServiceLinkServer\deployments` directory.
  - Step 4** Copy the entire **ServiceLink.war** sub-directory from this machine to the IIS machine and place it under the `C:\inetpub\WAR\` directory.

### Clustered Wildfly installation with Two VM Topology

- 
- Step 1** On the WildFly machine that is the primary cluster node for **RequestCenter**, **cd** to the `<PSC_Install_Dir>\wildfly-10.1.0.Final\content` directory.
  - Step 2** Copy the entire **RequestCenter.war** sub-directory from this machine to the IIS machine, and place it under the `C:\inetpub\WAR\` directory.

- Step 3** On the same WildFly machine, **cd** to the `<PSC_Install_Dir>\wildfly-10.1.0.Final\content` directory.
- Step 4** Copy the entire **ISEE.war** sub-directory from this machine to the IIS machine and place it under the `C:\inetpub\WAR` directory.
- Step 5** Rename the folder to `C:\inetpub\WAR\ServiceLink.war`.

## Create Virtual Directories for IIS

- 
- Step 1** On the IIS machine, launch **Internet Information Services (IIS) Manager**.
  - Step 2** Choose **Hostname > Sites > Default Web Site**.
  - Step 3** Right click on the **Default Web Site** and select **Add Virtual Directory**.
  - Step 4** On the pop up window, enter the following values, and then click **OK**:  
 Alias = RequestCenter  
 Physical path = <Click the browse button, and select the "C:\inetpub\WAR\RequestCenter.war" directory.>
  - Step 5** Right click on **Default Web Site** and select **Add Virtual Directory** to add another directory.
  - Step 6** On the pop up window, enter the following values, and then click **OK**:  
 Alias = IntegrationServer  
 Physical path = <Click the browse button, and select the "C:\inetpub\WAR\ServiceLink.war" directory.>
  - Step 7** Right click on **Default Web Site** and select **Add Virtual Directory** to add another directory.
  - Step 8** On the display window, enter the following values, and then click **OK**:  
 Alias = tomcat  
 Physical path = C:\inetpub\isapi
  - Step 9** Click on **Default Web Site** node. And on the right pane, double click **ISAPI Filters**.
  - Step 10** Click **Add** link under the **Actions** column on the right pane.
  - Step 11** On the pop up window, enter the following values, and then click **OK**:  
 Filter name = tomcat  
 Executable = C:\inetpub\isapi\isapi\_redirect.dll
  - Step 12** Click on **Default Web Site** node. And on the right panel, double click **Handler Mappings**.
  - Step 13** Click the **Edit Feature Permissions** link under the **Actions** column on the right pane.
  - Step 14** On the pop up window, select **all Read, Script** and **Execute** check boxes, and then click **OK**.
  - Step 15** Click on the **Hostname** node. On the right panel, double click on **ISAPI and CGI Restrictions**.
- 
-  **Note** The *Hostname* node is the parent node of sites.
- 
- Step 16** Click the **Add** link under the **Actions** column on the right most pane.
  - Step 17** On the display window, enter the following values, and then click **OK**:  
 ISAPI or CGI path = C:\inetpub\isapi\isapi\_redirect.dll  
 Description = Tomcat ISAPI Filter  
 Select the checkbox "Allow extension path to execute".

## Modify Plugin Properties

**Step 1** Modify the file `C:\inetpub\isapi\isapi_redirect.properties` as follows:

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/tomcat/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=C:\inetpub\isapi\logs\isapi_redirect.log
# Log level (debug, info, warn, error or trace)
log_level=error
# Full path to the workers.properties file
worker_file=C:\inetpub\isapi\conf\workers.properties
# Full path to the uriworkermap.properties file
worker_mount_file=C:\inetpub\isapi\conf\uriworkermap.properties
```

**Step 2** Modify the file `C:\inetpub\isapi\conf\uriworkermap.properties` as follows:

```
/RequestCenter=router1
/RequestCenter/*=router1
/RequestCenter/servlet/*=router1

/IntegrationServer=router2
/IntegrationServer/*=router2
/IntegrationServer/servlet/*=router2

/private/admin/jkstatus=jkstatus
```

**Step 3** If you have a standalone WildFly installation, then modify the file `C:\inetpub\isapi\conf\workers.properties` as follows:

```
# Define list of workers that will be used for mapping requests
worker.list=router1,router2,jkstatus

# Define Node1 worker for RequestCenter
worker.rcnode1.port=8009
worker.rcnode1.host=<IP_Address_of_RC_host>
worker.rcnode1.type=ajp13
worker.rcnode1.lbfactor=1
worker.router1.type=lb
worker.router1.balance_workers=rcnode1

# Define Node2 worker for ServiceLink
worker.rcnode2.port=6009
worker.rcnode2.host=<IP_Address_of_SL_host>
worker.rcnode2.type=ajp13
worker.rcnode2.lbfactor=1
worker.router2.type=lb
worker.router2.balance_workers=rcnode2

# Define a jkstatus worker using status
worker.jkstatus.port=8009
worker.jkstatus.host=<IP_Address_of_IIS_host>
worker.jkstatus.type=status
worker.status.type=status
```

The port numbers *8009* and *6009* should be set to the actual *ajp* port numbers used by the *RequestCenter* server and *ServiceLink* server.

**Step 4** If you have a clustered WildFly installation (regardless of 4-VM Topology or 2-VM Topology), then modify the file `C:\inetpub\isapi\conf\workers.properties` as follows:

**Note**

The following is an example for a WildFly installation with 2 cluster nodes of *RequestCenter*.

- That is there are 2 *RequestCenter* servers running on two separate VM's.
- If you have 3 or 4 cluster nodes, you just need to follow this example and add a section for *rcnode3* and for *rcnode4* appropriately.

```
# Define list of workers that will be used for mapping requests
worker.list=router1,router2,jkstatus

# Define Node1 worker for RequestCenter
worker.rcnode1.port=8009
worker.rcnode1.host=<IP_Address_of_RC1_host>
worker.rcnode1.type=ajp13
worker.rcnode1.lbfactor=1
worker.rcnode1.max_packet_size=65536

# Define Node2 worker for RequestCenter
worker.rcnode2.port=8009
worker.rcnode2.host=<IP_Address_of_RC2_host>
worker.rcnode2.type=ajp13
worker.rcnode2.lbfactor=1
worker.rcnode2.max_packet_size=65536

# Load-balancing behaviour
worker.router1.type=lb

# For clustering, set the line below to rcnode1, rcnode2 etc
worker.router1.balance_workers=rcnode1, rcnode2

# Define Node worker for SL
worker.slnode.port=6009
worker.slnode.host=<IP_Address_of_SL_host>
worker.slnode.type=ajp13
worker.slnode.lbfactor=1
worker.rcnode2.max_packet_size=65536
worker.router2.type=lb
worker.router2.balance_workers=slnode

# Define a 'jkstatus' worker using status
worker.jkstatus.port=8009
worker.jkstatus.host=<IP_Address_of_IIS_host>
worker.jkstatus.type=status
worker.jkstatus.max_packet_size=65536
worker.status.type=status
```

**Step 5** Restart **World Wide Web Publishing Service**.

**Step 6** If you have a standalone WildFly installation, skip to the section [Test IIS](#).

**Note**

If you have clustered Wildfly installation, continue to the next section [Configure instance-id for Wildfly](#).

# Configure Instance-ID for WildFly

## For 4 VM Topology

You must perform the following steps for clustered WildFly installation with 4 VM topology:

- 
- Step 1** Log on to the **WildFly Domain Controller** machine, and stop all WildFly servers.
- Step 2** Open file <PSC\_Install\_Dir>\wildfly-10.1.0.Final\domain\configuration\domain.xml and search for the following line:

```
<subsystem xmlns="urn:jboss:domain:undertow:3.1">
```

Replace it with the following value at two places within domain.xml:

```
<subsystem xmlns="urn:jboss:domain:undertow:3.1" instance-id="{jboss.web.instanceId}">
```

- Step 3** Log on to the **Host Controller 1 for RequestCenter**, and stop all WildFly servers.
- Step 4** Open file <PSC\_Install\_Dir>\wildfly-10.1.0.Final\domain\configuration\host1\_backup.xml, and search for the following section:

```
<servers>
<server name="server-host1-RC" group="main-server-group" auto-start="true">
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<!--<option value="-Xrunjdpw:transport=dt_socket,address=8787,server=y,suspend=n"/>-->
<option
value="-XX:CompileCommand=exclude,com/newscale/bfw/signon/filters,AuthenticationFilter"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0"/>
</server>
</servers>
```

Replace it with the following:

```
<servers>
<server name="server-host1-RC" group="main-server-group" auto-start="true">
<system-properties>
<property name="jboss.web.instanceId" value="rcnode1"/>
</system-properties>
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<!--<option value="-Xrunjdpw:transport=dt_socket,address=8787,server=y,suspend=n"/>-->
<option
value="-XX:CompileCommand=exclude,com/newscale/bfw/signon/filters,AuthenticationFilter"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option
```



```

value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr" />
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0" />
</server>
</servers>

```

**Step 5** Log on to the **Host Controller 2** for **RequestCenter**, and stop all Wildfly servers.

**Step 6** Open file <PSC\_Install\_Dir>\wildfly-10.1.0.Final\domain\configuration\host2\_backup.xml, and search for the following section:

```

<servers>
<server name="server-host2-RC" group="main-server-group" auto-start="true">
<jvm name="default">
<heap size="2048m" max-size="2048m" />
<permgen size="512m" max-size="512m" />
<jvm-options>
<!--<option value="-Xrunjdpw:transport=dt_socket,address=8787,server=y,suspend=n" />-->
<option
value="-XX:CompileCommand=exclude,com/newscaler/bfw/signon/filters,AuthenticationFilter" />
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement" />
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal" />
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal" />
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr" />
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0" />
</server>
</servers>

```

Replace it with the following:

```

<servers>
<server name="server-host2-RC" group="main-server-group" auto-start="true">
<system-properties>
<property name="jboss.web.instanceId" value="rcnode2" />
</system-properties>
<jvm name="default">
<heap size="2048m" max-size="2048m" />
<permgen size="512m" max-size="512m" />
<jvm-options>
<!--<option value="-Xrunjdpw:transport=dt_socket,address=8787,server=y,suspend=n" />-->
<option
value="-XX:CompileCommand=exclude,com/newscaler/bfw/signon/filters,AuthenticationFilter" />
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement" />
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal" />
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal" />
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr" />
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0" />
</server>
</servers>

```

**Note**

If you have more than 2 cluster nodes, then repeat [Step 5](#) and [Step 6](#) for each subsequent node. For example,

- On the 3rd node, you need to modify the file *host3\_backup.xml* and add the system-properties for *rcnode3*.
- On the 4th node, you need to modify the file *host4\_backup.xml* and add the system-properties for *rcnode4*.

**Step 7** Start up Wildfly servers on the **Domain Controller** machine and on each **Host Controller** machine.

**Step 8** Go to the section [Test IIS](#).

## For 2 VM Topology

Perform the steps in this section only if you have a clustered WildFly installation with 2 VM topology:

**Step 1** Log on to the **WildFly Domain Controller** machine, and stop all WildFly servers.

**Step 2** Open file `<PSC_Install_Dir>\wildfly-10.1.0.Final\domain\configuration\domain.xml` and search for the following line:

```
<subsystem xmlns="urn:jboss:domain:undertow:3.1">
```

Replace it with the following value at two places within domain.xml:

```
<subsystem xmlns="urn:jboss:domain:undertow:3.1" instance-id="${jboss.web.instanceId}">
```

**Step 3** Open file `<PSC_Install_Dir>\wildfly-10.1.0.Final\domain\configuration\hostva_backup.xml`, and search for the following section:

```
<servers>
<server name="server-host1-RC" group="main-server-group" auto-start="true">
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<!--<option value="-Xrunjdwp:transport=dt_socket,address=8787,server=y,suspend=n"/>-->
<option
value="-XX:CompileCommand=exclude,com/newscale/bfw/signon/filters,AuthenticationFilter"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0"/>
</server>
<server name="server-host1-SL" group="other-server-group" auto-start="true">
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<option value="-server"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="standard-sockets" port-offset="0"/>
</server>
</servers>
```

Replace it with the following:

```
<servers>
<server name="server-host1-RC" group="main-server-group" auto-start="true">
<system-properties>
<property name="jboss.web.instanceId" value="rcnode1"/>
</system-properties>
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<!--<option value="-Xrunjdpw:transport=dt_socket,address=8787,server=y,suspend=n"/>-->
<option
value="-XX:CompileCommand=exclude,com/newscall/bfw/signon/filters,AuthenticationFilter"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0"/>
</server>
<server name="server-host1-SL" group="other-server-group" auto-start="true">
<system-properties>
<property name="jboss.web.instanceId" value="slnode"/>
</system-properties>
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<option value="-server"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="standard-sockets" port-offset="0"/>
</server>
</servers>
```

**Step 4** Log on to the **Host Controller 2** for **RequestCenter**, and stop all WildFly servers.

**Step 5** Open file `<PSC_Install_Dir>\wildfly-10.1.0.Final\domain\configuration\host2_backup.xml`, and search for the following section:

```
<servers>
<server name="server-host2-RC" group="main-server-group" auto-start="true">
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<!--<option value="-Xrunjdpw:transport=dt_socket,address=8787,server=y,suspend=n"/>-->
<option
value="-XX:CompileCommand=exclude,com/newscall/bfw/signon/filters,AuthenticationFilter"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0"/>
</server>
```

```
</servers>
```

Replace it with the following:

```
<servers>
<server name="server-host2-RC" group="main-server-group" auto-start="true">
<system-properties>
<property name="jboss.web.instanceId" value="rcnode2"/>
</system-properties>
<jvm name="default">
<heap size="2048m" max-size="2048m"/>
<permgen size="512m" max-size="512m"/>
<jvm-options>
<!--<option value="-Xrunjdwp:transport=dt_socket,address=8787,server=y,suspend=n"/>-->
<option
value="-XX:CompileCommand=exclude,com/newscale/bfw/signon/filters,AuthenticationFilter"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xml/dtm/ref/sax2dtm/SAX2DTM,startElement"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option value="-XX:CompileCommand=exclude,org/exolab/castor/xml/Marshaller,marshal"/>
<option
value="-XX:CompileCommand=exclude,org/apache/xpath/compiler/XPathParser,UnionExpr"/>
</jvm-options>
</jvm>
<socket-bindings socket-binding-group="ha-sockets" port-offset="0"/>
</server>
</servers>
```



#### Note

If you have more than 2 cluster nodes, then repeat [Step 4](#) and [Step 5](#) for each subsequent node. For example,

- On the 3rd node, you need to modify the file *host3\_backup.xml* and add the system-properties for *rcnode3*.
- On the 4th node, you need to modify file *host4\_backup.xml* and add the system-properties for *rcnode4*.

**Step 6** Start up WildFly servers on the **Domain Controller** machine and on the **Host Controller 2** machine.

**Step 7** Go to the section [Test IIS](#).

## Test IIS

The following section provides information on verifying the connection to Prime Service Catalog.

**Step 1** Verify by connecting to the URL **[http://<IP\\_Address\\_of\\_IIS\\_Host>/RequestCenter](http://<IP_Address_of_IIS_Host>/RequestCenter)**.

If you connected you can see the Login Page of Prime Service Catalog.

**Step 2** For clustered WildFly installation with 2 nodes, stop one of the nodes.

And verify that you can still connect to the URL **[http://<IP\\_Address\\_of\\_IIS\\_Host>/RequestCenter](http://<IP_Address_of_IIS_Host>/RequestCenter)**.

# Configuring Data Source for SQL in WildFly

**Step 1** Log on to the WildFly Admin console (URL example below) with you credentials and click **OK**. This will take you to WildFly Application administrator console.

URL example:

<http://<hostname>:<port>/RequestCenter>

where,

<hostname> = The fully qualified domain hostname or the IP address of the computer where you installed the WildFly server for Service Catalog.

<port> =The HTTP Port number assigned to the Wildfly server for Service Catalog. The default value for HTTP Port number is 8080.

**Step 2** Click on **Configuration** tab to be able to edit and make changes.

**Step 3** Click **Add** to add a new data source.

**Step 4** Enter **Name:** **SERVICECATALOGDS** and **JNDI Name:** **java:/<Name of the data source>**

**Step 5** Click **Next**

**Step 6** Select driver as “**Microsoft**” and click **Next**.

**Step 7** Enter the connection URL: **jdbc:sqlserver://<db\_server>:1433;DatabaseName=VM236\_RCDB\_RC4**

**Step 8** Enter your credentials.

**Step 9** Fill up the various fields under different tabs as mentioned in the table below:

Tab Name	Fieldname	Value
Security	Secure Domain	CiscoSecureDataSource
Connection	<b>Use JTA and Use CCMsSECURITY</b>	Both these options should be checked.
Properties	1. SelectMethod:  2. sendStringParametersAsUnicode:	1. Direct  2. True
Pool	Minimum size is 20, maximum size is 80 and other values set to False.	
Validation		
	Background Validation	False
	Validation Millis	90000
	Validate on Match	False

**Step 10** Click **Enable > Confirm**.

**Note**

(Applicable only for WildFly cluster) If the datasource is still disabled, set the datasource to `<enabled = true>` in domain.xml file and restart the domain.

- Step 11** In the Connection Tab test the connection and you will see the confirmation message: “Successfully created the JDBC connection.”
- Step 12** Restart the WildFly server.

## Configuring Data Source for Oracle in WildFly

- Step 1** Log on to the WildFly Admin console (URL example below) with your credentials and click **OK**. Click on **Configuration** tab to be able to edit and make changes.

URL example:

<http://<hostname>:<port>/RequestCenter>

where,

`<hostname>` = The fully qualified domain hostname or the IP address of the computer where you installed the WildFly server for Service Catalog.

`<port>` = The HTTP Port number assigned to the Wildfly server for Service Catalog. The default value for HTTP Port number is 8080.

- Step 2** Click **Add** to add a new data source.
- Step 3** Enter **Name:** **SERVICECATALOGDS** and **JNDI Name:** **java:/<Name of the data source>**
- Step 4** Click **Next**
- Step 5** Select driver as “**oracle-thin**” and click **Next**.
- Step 6** Enter the connection URL:  
jdbc:oracle:thin:@//<db\_server>:1433;DatabaseName=VM236\_RCDB\_RC4
- Step 7** Enter your credentials.
- Step 8** Fill up the various fields under different tabs as mentioned in the table below:

Tab Name	Fieldname	Value
Security	Secure Domain	CiscoSecureDataSource
Connection	<b>Use JTA and Use CCM</b>	Both these options should be checked.
Properties	1. SelectMethod:  2. sendStringParametersAsUnicode:	1. Direct  2. True

Pool	Minimum size is 20, maximum size is 80 and other values set to False.	
Validation		
	Background Validation	False
	Validation Millis	90000
	Validate on Match	False

**Step 9** Click **Enable > Confirm**.



**Note**

(Applicable only for WildFly cluster) If the datasource is still disabled, set the datasoure to <enabled = true> in domain.xml file and restart the domain.

**Step 10** In the Connection Tab test the connection and you will see the confirmation message: "Successfully created the JDBC connection."

**Step 11** Restart the WildFly server.







## Port Usage for Prime Service Catalog

This chapter covers the standard ports used by Prime Service Catalog during installation. For the specific application it must be ensured that the ports listed in the table [Port Information](#) are open. You can also refer to the `csp.properties` file located at `C:\<Install_Directory>` for most the ports used in the system.

All the authorized ports come with the configuration file (`standalone-full.xml` or `domain.xml`) that comes with the particular version of Wildfly. These can be viewed by clicking the button during the installation process.



**Note**

All other ports can be protected by firewalls such as, iptables,

**Table C-1** *Port Information*

<b>App/Web Servers</b>	<b>Port Numbers</b>
Web Server Tier	If the webserver is hosted on same server as the application server <ul style="list-style-type: none"><li>• 80 for HTTP</li><li>• 443 for HTTPS</li></ul>
Application Server Tier	<ul style="list-style-type: none"><li>• 8080 (HTTP) and 8443 (HTTPS) for direct access to the application server</li><li>• 8009 for AJP connection from web tier, if web tier is hosted on separate server</li><li>• 6080 (HTTP) and 6443 (HTTPS) for Service Link if is on a separate host from Service Catalog</li><li>• 6009 for AJP connection from Service Link if is on a separate host from Service Catalog</li></ul>
Reporting Web Server	80 and/or 443
Database	<ul style="list-style-type: none"><li>• 1433 for MS-SQL</li><li>• 1521 for Oracle</li></ul>

App/Web Servers	Port Numbers
Management Console	For RC <ul style="list-style-type: none"> <li>• 9990: Management HTTP port</li> <li>• 9993: Management HTTPS port</li> <li>• 9999: management.native.port</li> </ul> For SL <ul style="list-style-type: none"> <li>• 7990: Management HTTP port</li> <li>• 7443: Management HTTPS port</li> <li>• 7999: management.native.port</li> </ul>
IBM Cognos	9300 9362 9399
Weblogic	7001 8001 9001
RabbitMQ	15672
JMS message and queue configuration ports	RC_APPSERVER_JACORB_PORT=3528 RC_APPSERVER_JACORB_SSL_PORT=3529 RC_APPSERVER_MANAGEMENT_OSGI_HTTP_PORT=8090 RC_APPSERVER_MESSAGING_PORT=5445 RC_APPSERVER_MESSAGING_THROUGHPUT_PORT=5455 RC_APPSERVER_TXN_RECOVERY_ENVIRONMENT_PORT=4712 RC_APPSERVER_TXN_STATUS_MANAGER_PORT=4713 SL_APPSERVER_JACORB_PORT=2528 SL_APPSERVER_JACORB_SSL_PORT=2529 SL_APPSERVER_MANAGEMENT_OSGI_HTTP_PORT=6090 SL_APPSERVER_MESSAGING_PORT=3445 SL_APPSERVER_MESSAGING_THROUGHPUT_PORT=3455 SL_APPSERVER_TXN_RECOVERY_ENVIRONMENT_PORT=3712 SL_APPSERVER_TXN_STATUS_MANAGER_PORT=3713 RC_JNDI_PORT=6080