

CA Automation Suite for Clouds Base Configuration

Implementation Guide
Release 1.7.1



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This documentation set references the following CA Technologies products and components:

- CA Service Catalog
- CA Process Automation
- CA Embedded Entitlements Manager (CA EEM)
- CA Server Automation
- CA Business Intelligence
- CA IT Client Manager

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: Introduction	9
Chapter 2: Pre-installation Requirements	11
Review the System Architecture	12
Review System and Hardware Requirements	14
Review Interdependency Chart.....	16
Review Implementation Best Practices.....	16
Plan Components Installation	17
Installation Worksheet	19
Access Information for CA Products.....	23
Chapter 3: Install the Components	25
Install CA EEM	26
Review the Prerequisites	27
Install CA EEM	27
Verify Installation	31
(Optional) Configure CA EEM	32
Verify Users and User Groups	34
Install CA Business Intelligence	37
Create CA Business Intelligence Database	38
Create DSN and ODBC Connection	41
Install CA Business Intelligence	50
Verify Installation	72
Install CA Process Automation	74
Review the Prerequisites	76
Prepare Microsoft SQL Server	77
Install Third-Party Prerequisites.....	78
Install CA Process Automation	85
Verify Installation	105
Verify CA EEM Application and Users	106
Install CA ITCM	110
Install CA Server Automation	111
Review Prerequisites.....	112
Install CA Server Automation	113
Verify Installation	132
Install CA Service Catalog	134

Review the Prerequisites	135
Install CA Service Catalog	136
Run Setup Utility	141
Verify Installation	151
Apply Patches	152
Chapter 4: Configure the Components	153
Integrate CA Service Catalog with CA Server Automation	154
Integrate CA Service Catalog with CA Process Automation	155
Update Load Balancer Details	160
Configure CA Process Automation with Active Directory Server	160
Add an SSL Certificate to CA Process Automation	161
Configure CA Process Automation for ssl	163
Configure Custom Provisioning Process in CA Process Automation	163
Disable Default CA Service Catalog Rules	165
Configure Touchpoint in CA Server Automation	167
Configure Network in CA Server Automation	170
Configure Network Pool Access to Organizational Units	171
Configure CA Automation Suite for Clouds Foundation	172
Import CA Automation Suite for Clouds Foundation Content Pack	174
Verify CA Automation Suite for Clouds Foundation Content Import	176
Configure Default Cancellation State	178
Configure CA Process Automation Datasets	179
Configure CA Service Catalog Credentials	184
Integrate CA Process Automation with CA Server Automation	188
Configure CA Automation Suite for Clouds Base Configuration for ESX	189
Import CA Automation Suite for Clouds Base Configuration for ESX Content Pack	191
Configure CA Process Automation Datasets for ESX	199
Managing Virtual Machines in VMware ESX	208
Integrate CA Business Intelligence with CA Service Catalog	234
Prerequisites for CA Business Intelligence Integration with CA Service Catalog	234
Create DSN and ODBC Connection for CA Service Catalog	235
Import CA Service Catalog Reports	244
Configure CA Business Intelligence in CA Service Catalog	247
Configure Trusted Authentication	248
Verify the Integration	249
Integrate CA Business Intelligence with Active Directory	251
Prerequisites for CA Business Intelligence Integration with Active Directory	251
Configure CA Business Intelligence for LDAP Authentication	252
Verify the Integration	256
Configure CA IT Client Manager Software Delivery	257

Import Software Delivery Packages	257
Create a Software Delivery Package to deploy Batch Files	258
Create a Software Delivery Package to Install an MSI Program.....	261
CA IT Client Manager Installation and Configuration.....	262
Install Windows Automated Installation Kit.....	264
Create and Register Boot Images.....	265
Chapter 5: Upgrade to the Current Release	275
Upgrade from Release 1.7	275
Review the Prerequisites	276
Apply CA Service Catalog Patches	276
Upgrade Content.....	277
Post Upgrade Configuration.....	283
Upgrade from Release 1.6 SP01	290
Review the Prerequisites	291
Access the Published Service Offering in CA Service Catalog r12.7	291
Upgrade CA Service Catalog.....	292
Upgrade Content.....	295
Post Upgrade Configuration.....	301
Chapter 6: Uninstall the Solution	315
Uninstall CA Automation Suite for Clouds Base Configuration for ESX.....	315
Delete Data Views.....	316
Uninstall Content Packs	316
Remove CA Process Automation Content.....	317
Remove plugin.jar Files from CA Service Catalog.....	317
Remove CA EEM groups from CA EEM.....	317
Remove Storage Tables from Database	318
Uninstall CA Automation Suite for Clouds Foundation	318
Uninstall Content Pack	319
Remove CA Process Automation Content.....	319
Enable CA Service Catalog Default Rules	319
Remove plugin.jar Files from CA Service Catalog.....	320
Remove CA EEM groups from CA EEM.....	321
Chapter 7: Create a Reporting Dashboard	323
Review the Prerequisites.....	324
Create the ODBC Database Connection	324
Create DSN on the CA Server Automation Server.....	324
Create DSN on CA Business Intelligence Server	327

Import the BIAR file	327
Verify the BIAR File Import.....	328
Integrate CA Service Catalog with BusinessObjects Enterprise	328
Set and Test Administration Configuration Parameters	329
Configure Trusted Authentication	330
Run Predefined Reports	331
Administer Dashboards	331
Configure Content Elements	332
Sample URLs.....	333
Add Dashboards	334
Chapter 8: Troubleshooting	337
Software Package Added in CA IT Client Manager is Not Updated in CA Server Automation	337
Event Receiver is not Triggered.....	338
CA Business Intelligence Server Not Found or Down.....	338
Appendix A: Active Directory Configuration	341
How to Add the Active Directory Certification Role to Active Directory.....	341
How to Create an AD Certificate File.....	350
Appendix B: Security Configuration	359
Allow Remote Connections through Windows Firewall.....	359
Turn off Internet Explorer Enhanced Security Configuration.....	359
Turn on Windows 2008 Firewall.....	360
Enable Notifications	360
Allow Access.....	360
Allow ICMP	360
Appendix C: SQL Configuration	363
Install Microsoft SQL Server 2008 R2 Standard.....	363
Install SQL Server 2008 R2 Standard Client.....	365
Verify SQL Connectivity	372
How to Create an SQL Alias.....	373
How to Determine the TCP/IP Port Number for a Named Instance of SQL	374
Appendix D: Upgrade CA ITCM r12.8 C1	377

Chapter 1: Introduction

This guide describes the processes for a Service Provider to configure the CA Automation Suite for Clouds Base Configuration with the CA Automation Suite for Clouds Foundation.

CA Automation Suite for Clouds Base Configuration is a set of integrated CA Products that when combined with prebuilt content gives clients an operational server provisioning solution. CA Automation Suite for Clouds Base Configuration offers a simple user interface for ordering and approving new servers. An approved virtual server is automatically built, customized, and loaded with software based on the user requirements.

CA Automation Suite for Clouds Base Configuration base model includes the capabilities of CA Service Catalog, CA Process Automation, CA EEM, CA Business Intelligence, and CA Server Automation products. This base model is a starter pack if you do not have CA Server Automation but would like to take advantage of its capabilities.

Chapter 2: Pre-installation Requirements

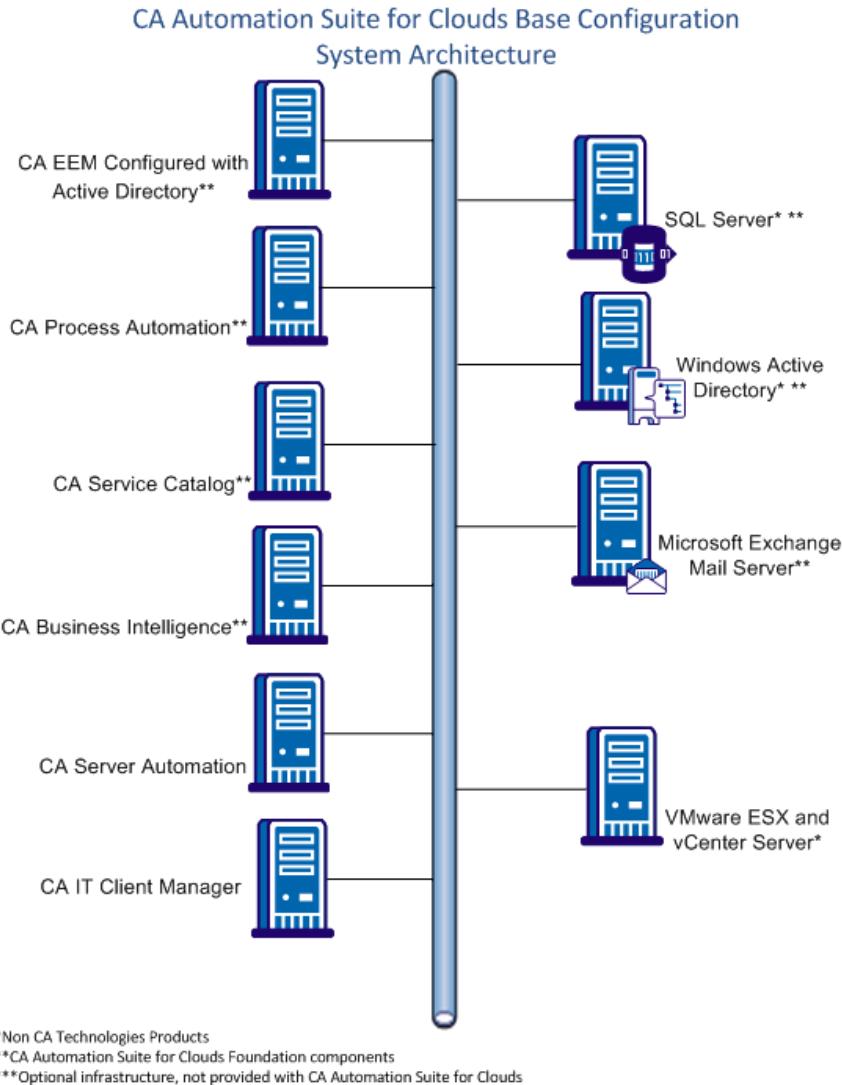
Before you begin installing the solution components, be sure to review the information in this chapter.

This section contains the following topics:

- [Review the System Architecture](#) (see page 12)
- [Review System and Hardware Requirements](#) (see page 14)
- [Review Interdependency Chart](#) (see page 16)
- [Review Implementation Best Practices](#) (see page 16)
- [Plan Components Installation](#) (see page 17)
- [Installation Worksheet](#) (see page 19)
- [Access Information for CA Products](#) (see page 23)

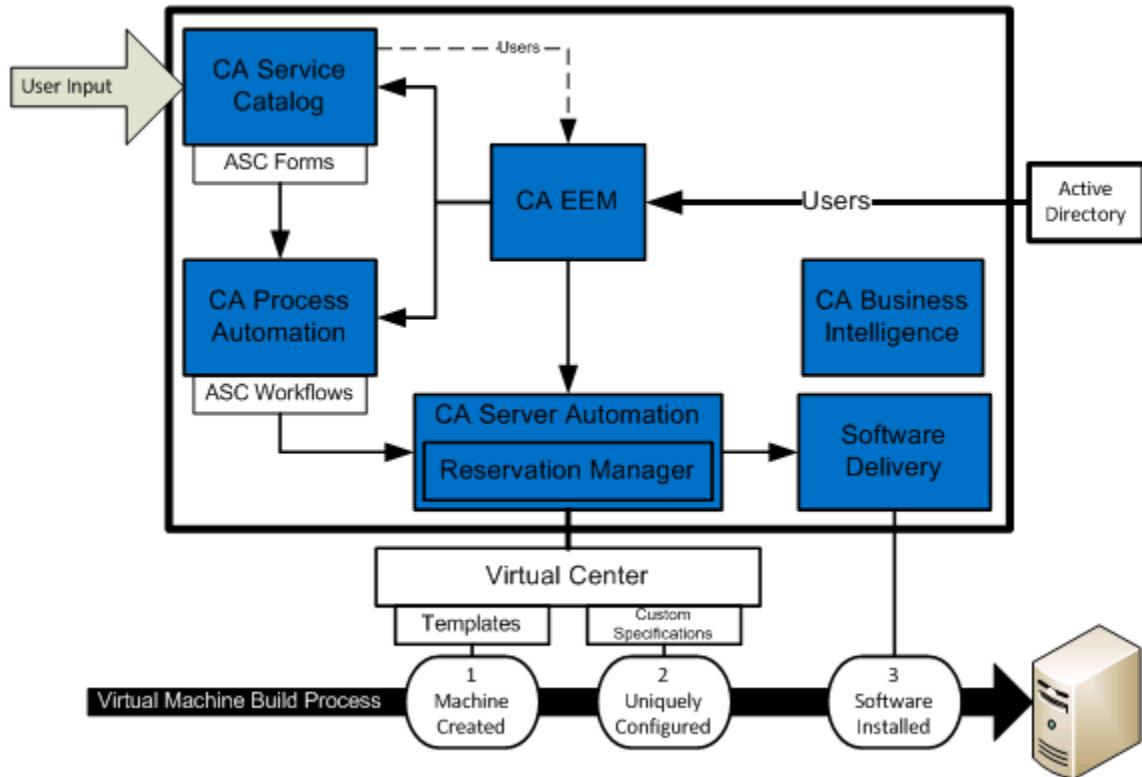
Review the System Architecture

The following graphic illustrates the high-level system architecture for the CA Automation Suite for Clouds Base Configuration:



The following flowchart shows how the CA Automation Suite for Clouds components works together to build and customize a new server:

CA Automation Suite for Clouds Base Configuration Architecture



Review System and Hardware Requirements

The following table provides the minimum system and hardware requirements for the solution:

Product Name	Product Version and Patches	Platform OS SP Level	Memory, CPU	Disk Space
CA Service Catalog	r12.8 CP03 with RO70135 patch	Microsoft Windows Server 2008 R2 x64 Standard Edition	4-GB RAM 2x vCPU	80 GB
CA Process Automation	r4.1 SP1 or r4.2 SP1	Microsoft Windows Server 2008 R2 x64 Standard Edition	4-GB RAM 2x vCPU	80 GB
CA EEM	r12.5 CR1	Microsoft Windows Server 2008 R2 x64 Standard Edition	4-GB RAM 2x vCPU	80 GB
CA Business Intelligence	r3.3	Microsoft Windows Server 2008 R2 x64 Standard Edition	4-GB RAM 2x vCPU	80 GB
CA Server Automation	r12.8.2	Microsoft Windows Server 2008 R2 x64 Standard Edition	8-GB RAM 2x vCPU*	80 GB
CA IT Client Manager	r12.8 C1	Microsoft Windows Server 2008 R2 x64 Standard Edition	8-GB RAM 2x vCPU	80 GB
VMware vCenter	vSphere Virtual Center 5.0 or vSphere Virtual Center 5.5	Microsoft Windows Server 2008 R2 x64 Standard Edition	8-GB RAM 2x vCPU	80 GB

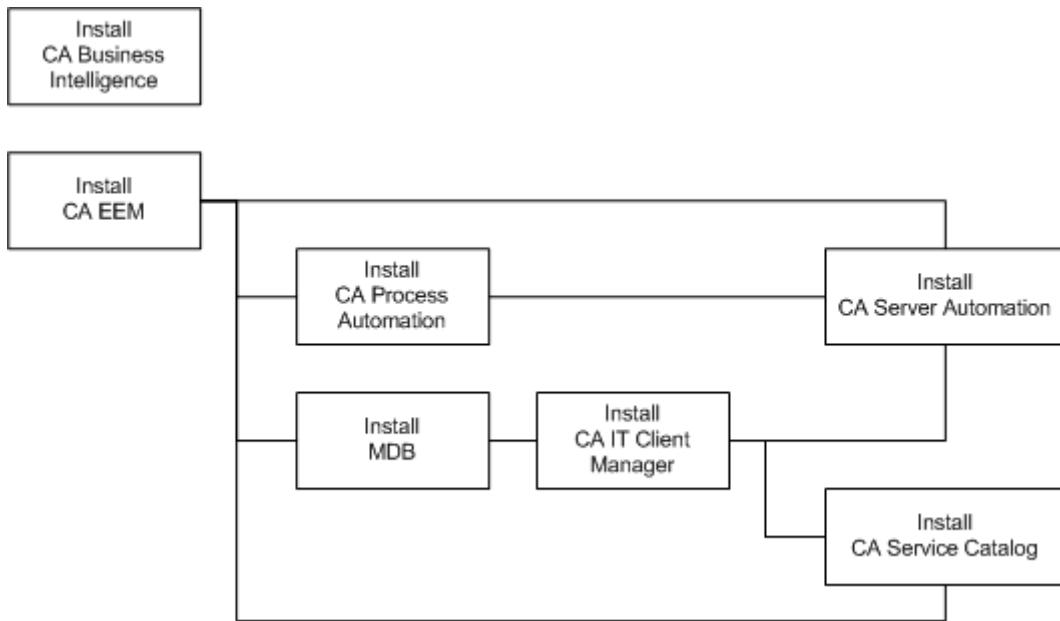
Product Name	Product Version and Patches	Platform OS SP Level	Memory, CPU	Disk Space
Microsoft SQL Server for following databases:	SQL Server 2008 R2 SP2 <ul style="list-style-type: none"> ■ CA Server Automation ■ CA MDB ■ CA Process Automation ■ CA Business Intelligence 	Microsoft Windows Server 2008 R2 x64 Standard Edition	8 GB 4x vCPU	80 GB

* Processor Speed per Server: Intel Xeon 51xx 2.6 GHz or equivalent, or Intel Core 2 Duo 2.6 GHz or equivalent.

Note: Install the patches in the same order that is mentioned in the Plan Components Installation section.

Review Interdependency Chart

The following chart shows the interdependencies that are based on the installation process:



Review Implementation Best Practices

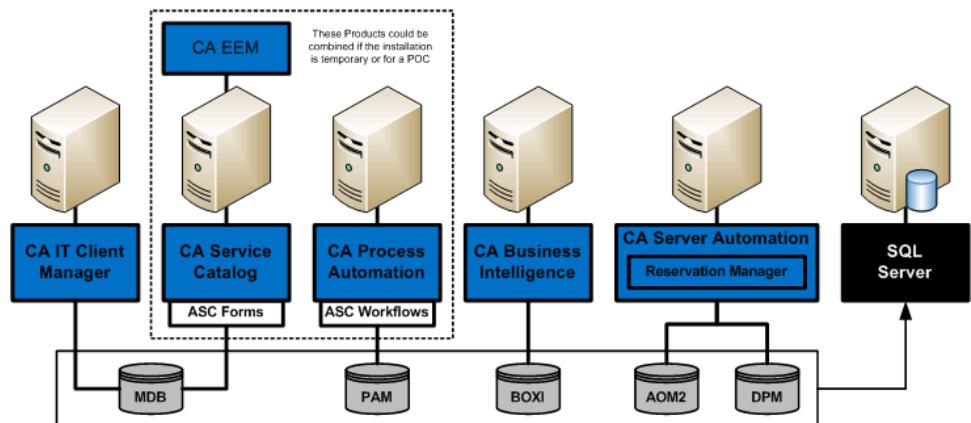
Before you start the installation process, we recommend the following steps to ensure a successful installation and implementation:

- Turn off Windows Firewalls. If this recommendation is not acceptable in your organization, then set the Windows Firewalls to Notify. The Notify setting informs you when a port or application is blocked so that you have the opportunity to create a Rule to permit access. For more information, see [Windows Firewall](#) (see page 360) in the Appendix section.

- Additionally, Windows Firewall by default blocks ICMP (PING) communication. We recommend that you turn off the option (if only temporarily). This option validates all the CA Automation Suite for Clouds servers can communicate with each other using Hostname (DNS Resolution) and IP Address.
- Add the user account that installs CA Automation Suite for Clouds as a member of the Local Administrators Group on each server. Perform this step even if your domain account is a domain administrator.
- Turn off Internet Explorer Enhanced Security Configuration. This setting allows all of the users to open the product web interfaces without having to set and configure access. For more information, see [Turn off Internet Explorer Enhanced Security Configuration](#) (see page 359).
- When installing on the Windows 2008 R2 operating system with a local administrative user ID, turn off User Account Control (UAC) for the installation process.

Plan Components Installation

We recommend that you install the CA Products and MS SQL Server database on different servers. The recommended production-type architecture for the CA Automation Suite for Clouds Base Configuration Base Model is as follows:



The following list provides a breakdown of the system components that are based on the server installation:

Server	CA Technologies Products
Server 1	CA EEM
Server 2	CA Business Intelligence
Server 3	CA Process Automation
Server 4	CA Server Automation
Server 5	CA Service Catalog <ul style="list-style-type: none">■ CA Service Catalog■ CA Service Accounting
Server 6	CA IT Client Manager

Prepare the [installation worksheet](#) (see page 19) before you begin installing the components.

The best practices for installing each CA Technologies product and performing the initial CA Automation Suite for Clouds post configurations are as follows:

Note: The following procedures assume that SQL Server is installed, and the SQL Client Tools are installed on each server.

Follow these steps:

1. [Install CA EEM](#) (see page 26).
2. [Install CA Business Intelligence](#) (see page 37).
3. [Install CA Process Automation](#) (see page 74).
4. [Install CA IT Client Manager](#) (see page 110).

5. Install and create the database (MDB) for Software Delivery and CA Service Catalog.
6. [Install CA Server Automation](#) (see page 111).
7. [Install CA Service Catalog](#) (see page 134).
8. [Perform CA Automation Suite for Clouds post configuration](#) (see page 153), including loading prebuilt content.
9. [Configure Software Delivery](#) (see page 257) for installing Software Packages.
10. Configure Reservation Manager and Virtual Center so that they can quickly and properly build virtual machines according to user specifications.

Installation Worksheet

The installation worksheet lets you take note of particular server names and credentials as you install each product. During some product installations and configurations, you provide specific data from other products such as server names, administrator credentials. You can refer to this worksheet to complete the required fields easily.

Local Computer Access

Local Administrator Account	
Local Administrator Account Password	

CA EEM

EEM Server Host Name	
EEM Administrator (EiamAdmin) Password	

Active Directory

Domain Controller Host Name	
Active Directory Port	389 (LDAP) or 3268 (GC – Global Catalog)
Domain Name (xyz.com)	
Base Domain Name (dc=xyz,dc=com)	
Domain Administrator (jdoe@xyz.com)	
User Domain Name (cn=jdoe,cn=users,dc=xyz,dc=com)	
Domain Administrator Password	

SQL Server

SQL Server Host Name	
SQL Port	1433
Named Instance	
Dynamic Port	
SQL Authentication (sa) User	
SQL Authentication User's Password	
Windows Authentication SQL User	
Windows Authentication SQL User's Password	

CA Business Intelligence/Objects (BOXI)

Host Name	
Administrator Password (blank)	

CMC Port	6400
Node Name	
Port	6410
Connection Port	8080
Shutdown Port	8005
Redirect Port	8443
Shared Secret	
CA Service Catalog ODBC Name	

CA Process Automation

Host Name	
Administrator Name (pamadmin)	
Administrator Password (pamadmin)	
Certificate Password	
Display Name	
Server Port	7001
HTTP Port	8080
JNDI Port	1099
RMI Port	1098
SNMP Port	162

CA Service Catalog

Host Name	
Administrator Name	spadmin
Administrator Password (spadmin)	

Installation Worksheet

MDB Administrator Name	usmuser
MDB Administrator Password	
Business Unit (case sensitive)	
Start-up Port (default 8080 MUST change)	8090
Shutdown Port	8095

CA IT Client Manager

Host Name	
Installer/Administrator and Password	/
CA IT Client Manager Database Administrator Password	
Tomcat Startup Port	8090
Tomcat Shutdown Port	8095
Tomcat ajp13 Port	8020

CA Server Automation

Host Name	
Network Discovery Gateway Port	8082
Service User ID (sys_system or admin)	
Service User Password	
Apache Port	443
Tomcat Server Port	8443
Tomcat Shutdown Port	8005
Apache ActiveMQ Message Broker Server Name	

Apache ActiveMQ Message Broker Port	61616
Virtual Center Server Host Name	
Virtual Center Administrator Name	
Virtual Center Administrator Password	
Virtual Center Port and Protocol	443 HTTPS
Windows Administrator Name and Password	/
Linux root User Name and Password	/
SNMP Read Community String	public
SNMP Read-Write Community String	snmp_admin
SystemEDGE Agent Port	161
SystemEDGE Agent Trap Community String	Public 127.0.0.1162
Remote Monitoring User Name and Password	/

Access Information for CA Products

Use the following links to access the various components of this solution:

CA EEM

<http://<CA EEM Server>:5250/spin/eiam/eiam.csp>

CA Process Automation

<http://<CA Process Automation Server>:8080/itpam>

CA Service Catalog

<http://<CA Service Catalog Server>:8080/usm/wpf>

CA Business Intelligence (BOXI Client Management Console)

<http://<BOXI Server>:8080/CmcApp>

CA Business Intelligence (BOXI Information View Application)

<http://<BOXI Server>:8080/InfoViewApp>

CA IT Client Manager (CA ITCM Software Delivery)

Access DSM Explorer (Client Tool)

CA Server Automation

<https://<Server Auto Server>:8443/UI>

Reservation Manager

<https://<Server Auto Server>:8443/ssrm>

Chapter 3: Install the Components

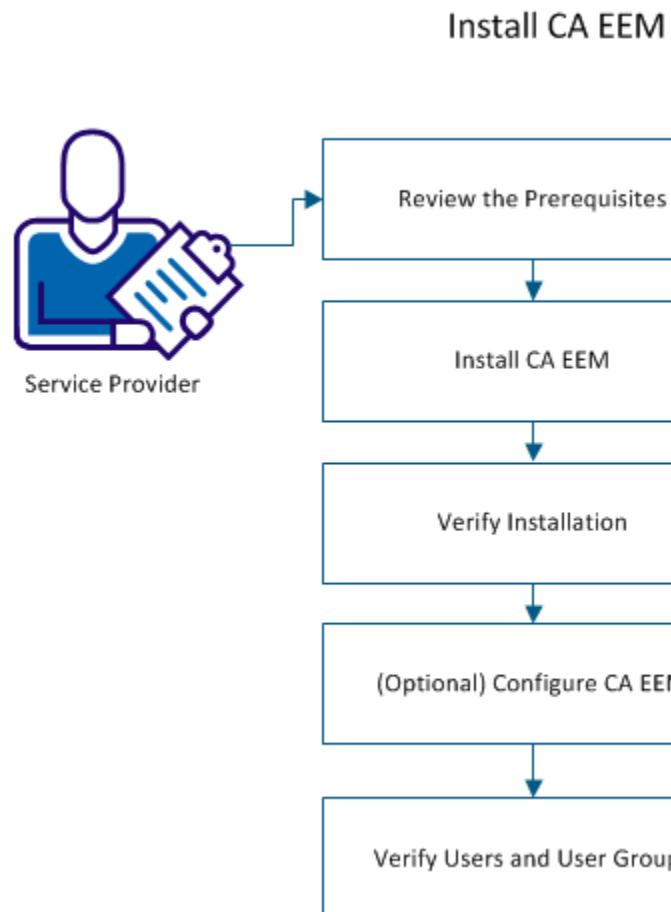
This chapter describes how to install CA Automation Suite for Clouds Base Configuration components.

This section contains the following topics:

- [Install CA EEM](#) (see page 26)
- [Install CA Business Intelligence](#) (see page 37)
- [Install CA Process Automation](#) (see page 74)
- [Install CA ITCM](#) (see page 110)
- [Install CA Server Automation](#) (see page 111)
- [Install CA Service Catalog](#) (see page 134)

Install CA EEM

CA EEM is a required component of CA Automation Suite for Clouds. CA EEM grants access to other solution components, such as CA Service Catalog, and CA Process Automation. CA EEM can be configured to stand alone or it can be integrated to use an external directory like Microsoft Active Directory.



To install this component, complete the following steps:

1. [Review the Prerequisites](#) (see page 27).
2. [Install CA EEM](#) (see page 27).
3. [Verify Installation](#) (see page 31).
4. [\(Optional\) Configure CA EEM](#) (see page 32).
5. [Verify Users and User Groups](#) (see page 34).

Review the Prerequisites

Refer to the Review System and Hardware Requirements section for general installation requirements. Complete and verify the following requirements before you begin the installation:

- [Review the recommended CA Automation Suite for Clouds architecture](#) (see page 12).
- Review the CA EEM section and the Microsoft Active Directory section of your [Installation Worksheet](#) (see page 19).
- Verify that Microsoft Active Directory is installed and running.
- If you plan to install CA Process Automation on this server, install Java JDK Version 1.7 or above (64 bit).

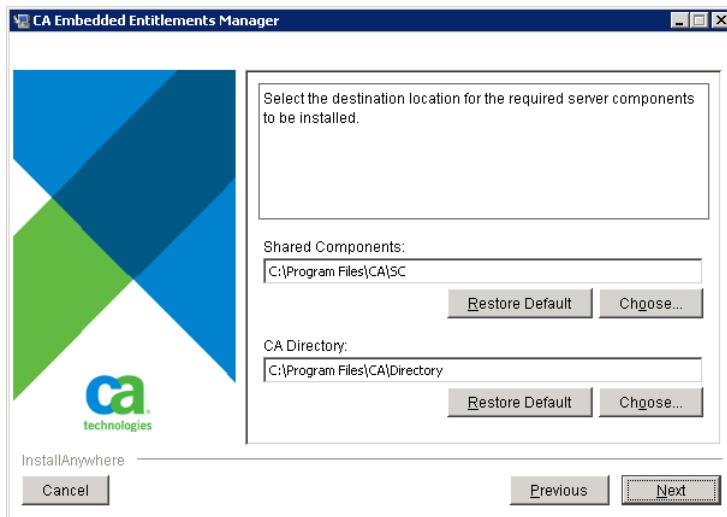
Install CA EEM

Perform the following steps to install CA EEM.

Note: As you step through these installation instructions, refer to the [Installation Worksheet](#) (see page 19) to find server names, file paths, login credentials, and port values. Use the given default values or note your changes on the worksheet.

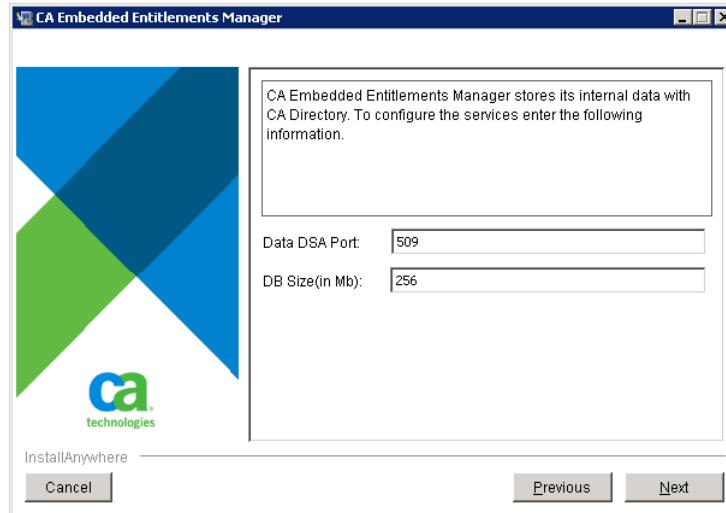
Follow these steps:

1. Log in to the CA EEM server as an administrator.
2. Extract the media to a folder on the target CA EEM server.
3. Execute EEMServer_12.51.1.8_win64.exe.
The Installation Wizard for CA EEM opens.
4. Click Next.
The License Agreement page opens.
5. Slide the scroll bar to the bottom of the page, select I accept the terms in the license agreements, and click Next.
The Destination Folder page opens.



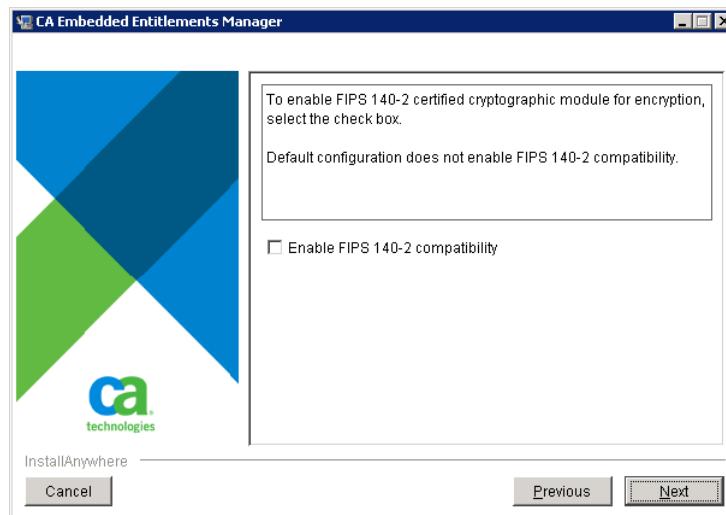
6. Verify the installation location, or click Choose to change the location.
7. Click Next.

The CA Directory Information page opens.



8. Accept the database information and click Next.
The CA EEM Password page opens.
9. Type Password, Confirm Password for EiamAdmin, and click Next.
Note: Record the EiamAdmin password in [Installation Worksheet](#) (see page 19).

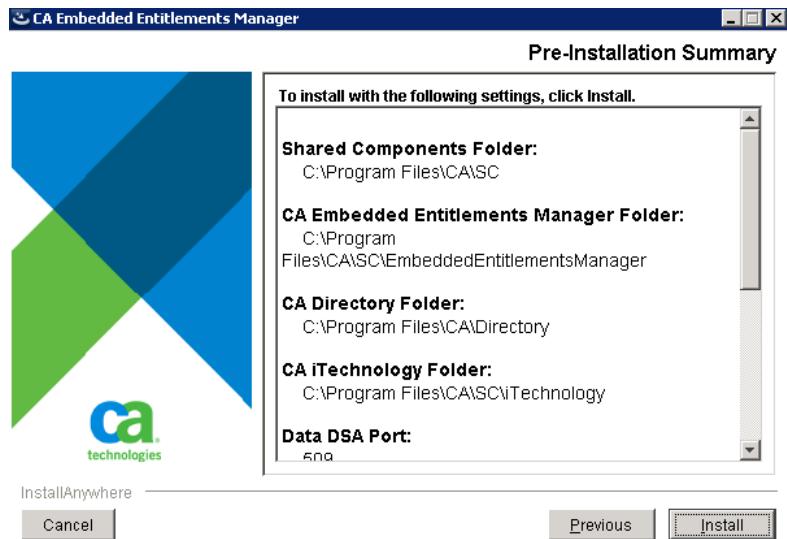
The FIPS security page opens.



10. Ensure that the *Enable FIPS140-2 compatibility* option is cleared and click Next.

Note: CA Automation Suite for Clouds uses MD5 as the default algorithm to encrypt and decrypt sensitive data.

The Installation Summary page opens.



11. Click Install.

The CA EEM installation begins and usually takes few minutes to complete.

The Installation Complete page opens.

12. Click Done.

The CA EEM installation is complete.

Verify Installation

Log in to CA EEM and verify that the component installed correctly.

Follow these steps:

1. Do *one* of the following tasks:
 - Select Start, All Programs, CA, Embedded Entitlements Manager, Admin UI.
 - Type `https://<EEM_Server>:<Port_Number>/spin/eiam` in a browser and press Enter.

The Login page opens.



2. Verify that Application is set to <Global>.
3. Log in to CA EEM as the Administrator (Default Admin Username: EiamAdmin).

If you can log in and access CA EEM, the installation was successful.

(Optional) Configure CA EEM

Configure CA EEM to use Microsoft Active Directory so that users can access the other components of CA Automation Suite for Clouds.

Note: Linking CA EEM with Microsoft Active Directory is not mandatory for CA Automation Suite for Clouds.

Follow these steps:

1. Access the CA EEM dashboard.
2. Click Configure, User Store.
3. Click User Store.

The Userstore Configuration page opens.



The screenshot shows the 'Userstore Configuration' page with the 'Global Users / Global Groups' tab selected. Under 'Directory Information', the 'Configuration Type' dropdown is set to 'Basic LDAP Directory'. The 'Reference from an external LDAP Directory' radio button is selected. There is a 'Save' and 'Close' button at the top right.

4. Select Reference from an external LDAP Directory.
5. Select Basic LDAP Directory in Configuration Type drop-down.
6. Click Add external LDAP directory.

The LDAP Directory Configuration page opens.



The screenshot shows the 'LDAP Directory Configuration' page with the 'General' tab selected. The 'Attribute Map' dropdown is set to 'Microsoft Active Directory'. Under 'Connection Settings', the 'Protocol' dropdown is set to 'LDAP'. There is a 'Save' and 'Close' button at the top right.

Note: Gather the necessary directory information beforehand to fill the form.

7. Complete the following fields and use the arrow to move the Host to the Selected Hostnames table.

Name

Specifies the LDAP directory name.

Attribute Map

Specifies the directory service that CA EEM uses.

Host

Specifies the host name of the domain controller. Host Name cannot be modified once assigned.

Port

Specifies the TCP port number for the Active Directory.

Default: 389 or 3268.

Protocol

Specifies the protocol that is used for communication.

Default: LDAP

Base DN (Domain Name)

Specifies the LDAP DN that is used as the base.

Note: No spaces are allowed.

Example: If the Domain Name is ASC-FORWARDINC.COM, type the following information:

DC=ASC-FORWARDINC,DC=COM

User DN

Specifies the DN used to attach to the external directory host.

Note: Enter the domain user only, domain administrator is not required.

Example: If the domain user name is Administrator, type the following information (spaces allowed):

CN=Administrator,CN=Users,DC=ASC-FORWARDINC,DC=COM

User Password and Confirm Password

Specifies the password for the User DN that is used to attach to the external directory host.

8. (Optional) Select host to delete and click the Bin icon to delete a connection to host.
9. (Optional) Use the arrows to move the host connection up/down the preference order.
10. Click Save.

A confirmation message appears. A list of available LDAP services appears in the Directory Information grid.

11. Click Close.

CA EEM is configured to use Microsoft Active Directory.

Verify Users and User Groups

Verify users and user groups in CA EEM so that users can access the necessary components of CA Automation Suite for Clouds.

Follow these steps:

1. Access the CA EEM home page.
2. Select Manage Identities, Users.

3. Complete the following details in the Search Users section and click Go.

Attribute

Specifies the attribute for the search.

Value: User Name

Operator

Specifies the operator type.

Value: LIKE

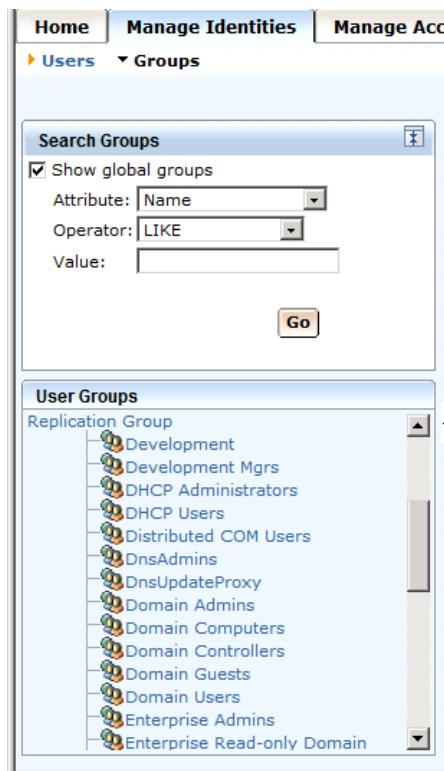
Value

Specifies the value for the search. Leave this field blank.

4. Verify that the Microsoft Active Directory users for your site appear in the Users section as shown in the following sample graphic and then select Groups.

The screenshot shows the CA EEM interface. At the top, there are tabs: Home (selected), Manage Identities, and Manage. Below the tabs, there is a navigation bar with 'Users' and 'Groups'. The main area is divided into two sections: 'Search Users' and 'Users'. The 'Search Users' section contains fields for Attribute (User Name), Operator (LIKE), and Value, along with a 'Go' button. The 'Users' section shows a tree view of users under the 'Users' folder, listing Admin, Administrator, ca, catalyst, catalystadmin, Guest, pamadmin, pamuser, and snadmin.

5. Do the following steps in the Search Groups section:
 - a. Select Show global groups.
 - b. Accept the default values for the Attribute, Operator, and Value fields, and click Go.
 - c. Verify that the Microsoft Active Directory user groups for your site appear in the User Groups section as shown in the following sample graphic.



6. Click Log Out to exit CA EEM.

The necessary users and user groups are in CA EEM.

You have installed CA EEM and configured it to use Microsoft Active Directory.

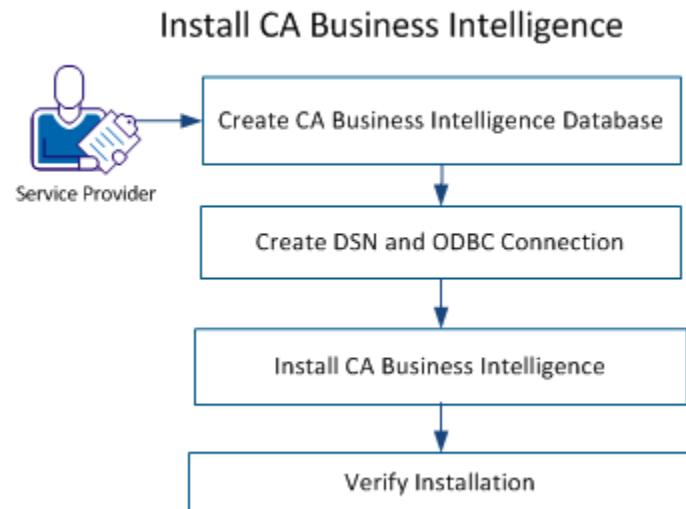
CA EEM manages your windows users. Enter other CA Automation Suite for Clouds domain users and assign them to the Local Administrator Group. Create the spadmin user for the CA Service Catalog. Create the pamadmin and pamuser users for CA Process Automation. Any CA application that leverages an authorization in CA EEM requires you to create the associated groups in the user store.

Install CA Business Intelligence

CA Business Intelligence is a set of reporting and analytic software that is used for presenting information and supporting business decisions. The solution uses CA Business Intelligence to integrate, analyze, and then present, through various reporting options.

CA Business Intelligence requires a database and ODBC connection before you can begin the installation.

The following diagram illustrates how a Service Provider installs the product and its components:



Follow these steps:

1. [Create CA Business Intelligence Database](#) (see page 38) in Microsoft SQL.
2. [Create DSN and ODBC Connection](#) (see page 41) for CA Business Intelligence Central Management System Database.
3. [Install CA Business Intelligence](#) (see page 50).
4. [Verify Installation](#) (see page 72).

Note: Complete the configuration of CA Business Intelligence after all products required for the Solution is installed.

Create CA Business Intelligence Database

You can create a Microsoft SQL database before installing CA Business Intelligence.

If MS SQL is installed on a different server, perform the following procedure on that server. However, since the MS SQL Client Tools are installed on the CA Business Intelligence server, it is recommended that you performed the steps remotely. Thus validates the SQL connectivity between the two servers.

Follow these steps:

1. Log in to the server where you want to install CA Business Intelligence.
2. Open Microsoft SQL Server Management Studio.

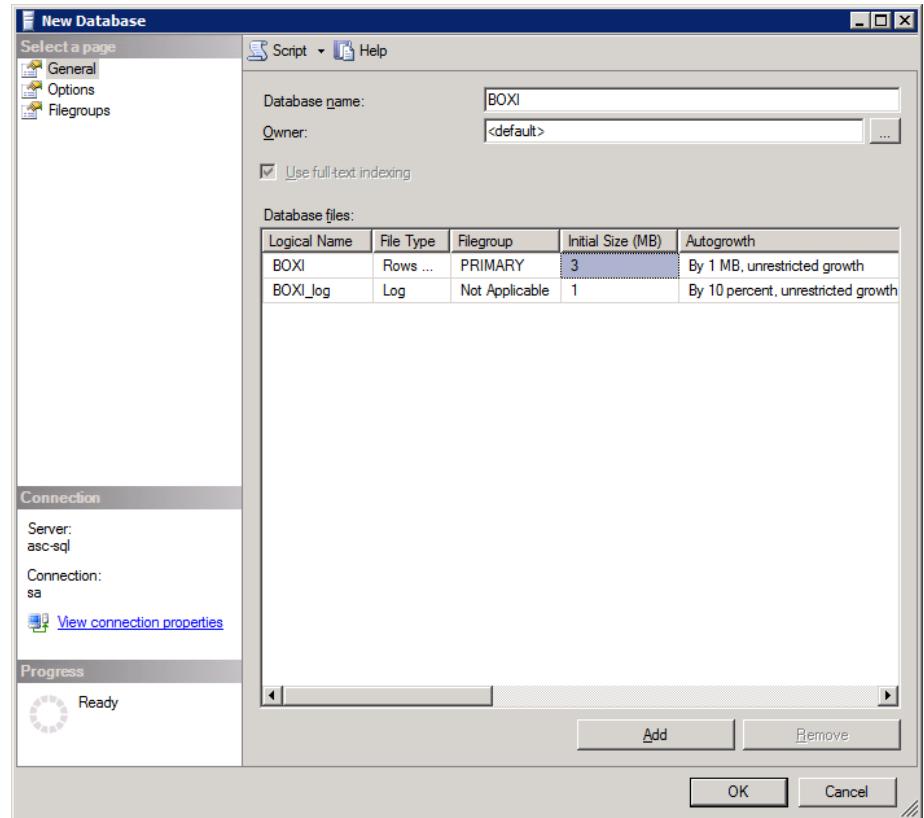
3. Log in using a SQL Administrator account (for example, sa).

The Microsoft SQL page opens.



4. Right-click Databases and select New Database.

The New Database dialog opens.



5. Click General in the Select a page panel.

The General dialog opens.

6. Enter a Database name (for example, BOXI) and click OK.

Note: Update your [Installation Worksheet](#) (see page 19) with the installation values. You need this information for subsequent installations.

You have created the CA Business Intelligence database in Microsoft SQL.

Create DSN and ODBC Connection

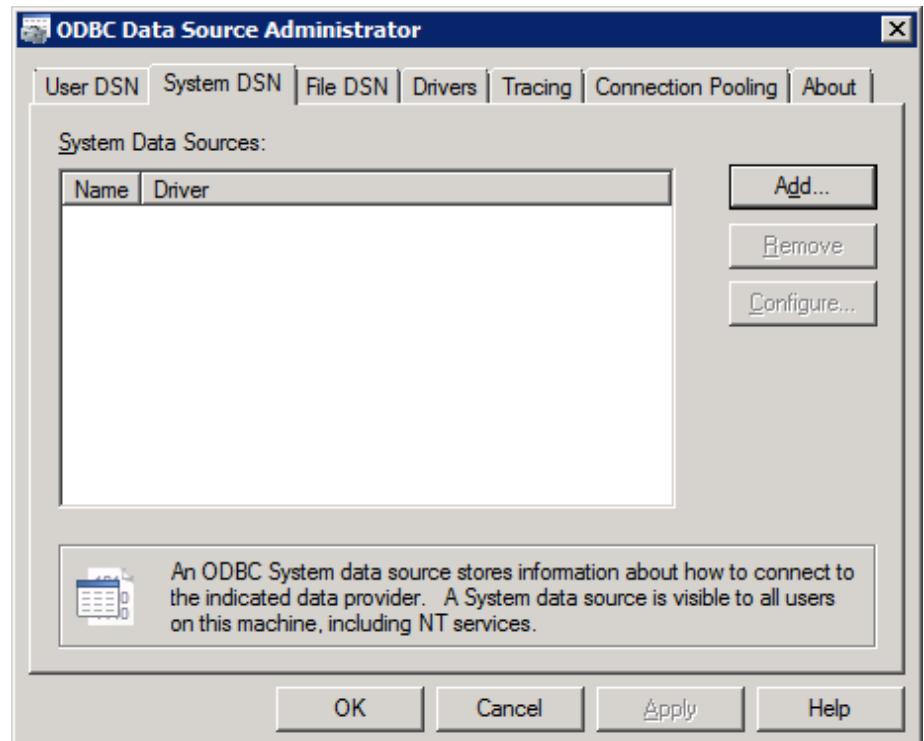
You can create an ODBC connection to the CA Business Intelligence Central Management Database.

Follow these steps:

1. Run the *odbcad32.exe* file from the following location:

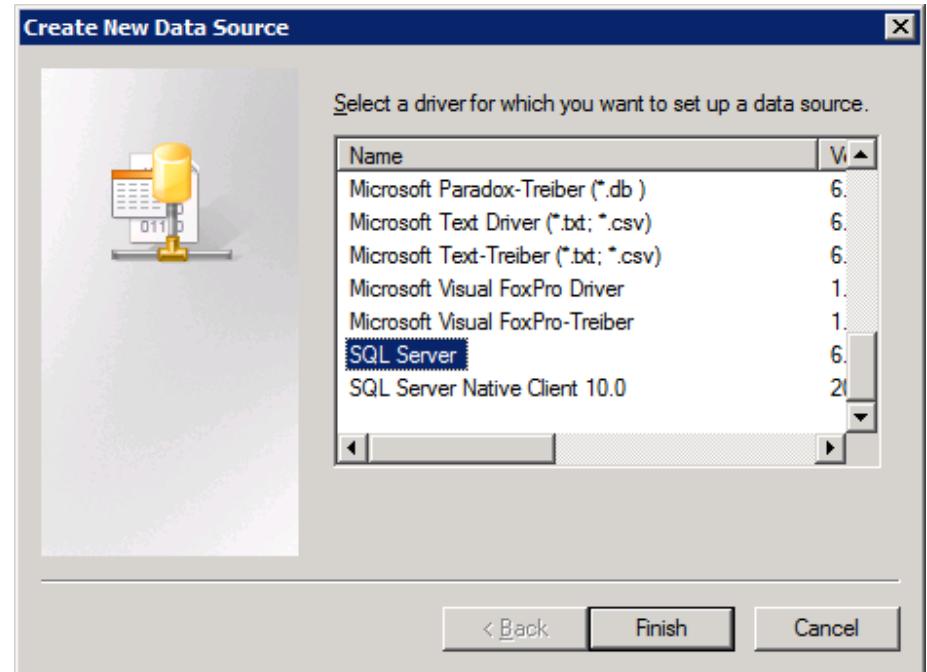
c:\Windows\SysWOW64\

The ODBC Data Source Administrator dialog opens.



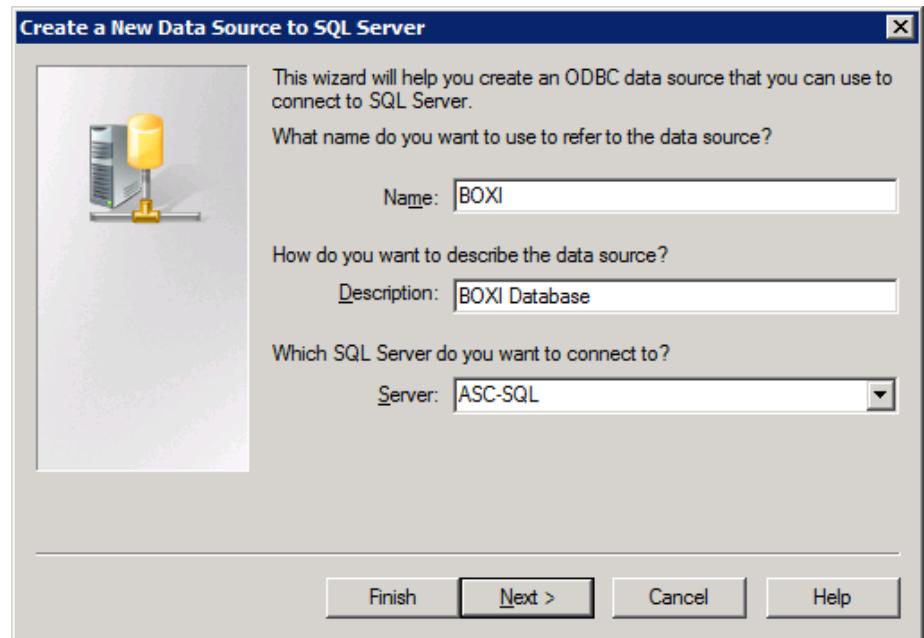
2. Click the System DSN tab, and click Add.

The Create New Data Source wizard opens.



3. Select SQL Server from the driver list and click Finish.

The *Create a New Data Source to SQL Server* page opens.



4. Enter the following parameters.

Name

Specifies the name of the database.

Example: BOXI

Description

(Optional) Specifies the description of the data source.

Example: Business Objects CMS Database

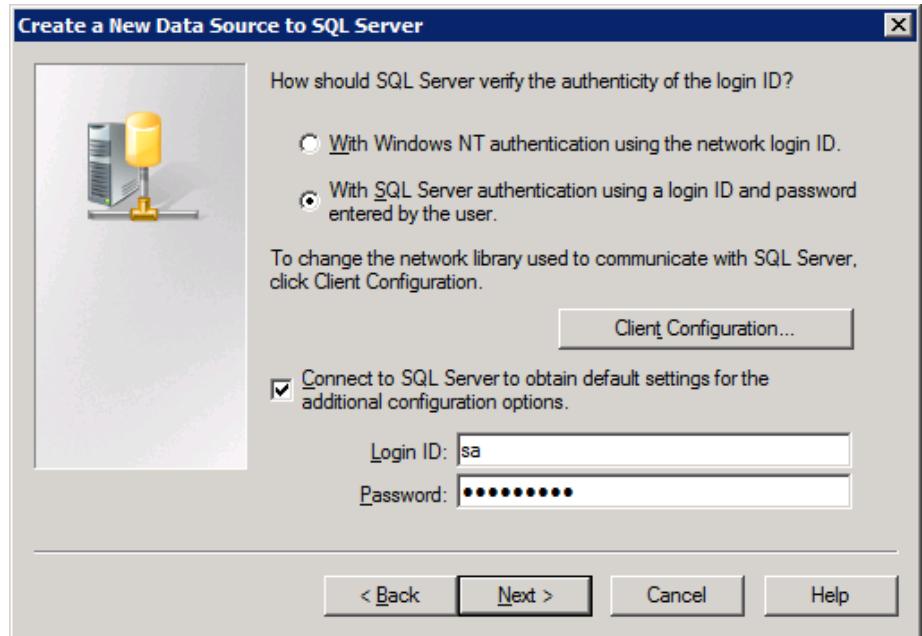
Server

Use the drop-down list and select the server where the database resides. If a Named Instance of SQL is used, then enter <SQL Server>\<Named Instance>.

Default: localhost

5. Click Next:

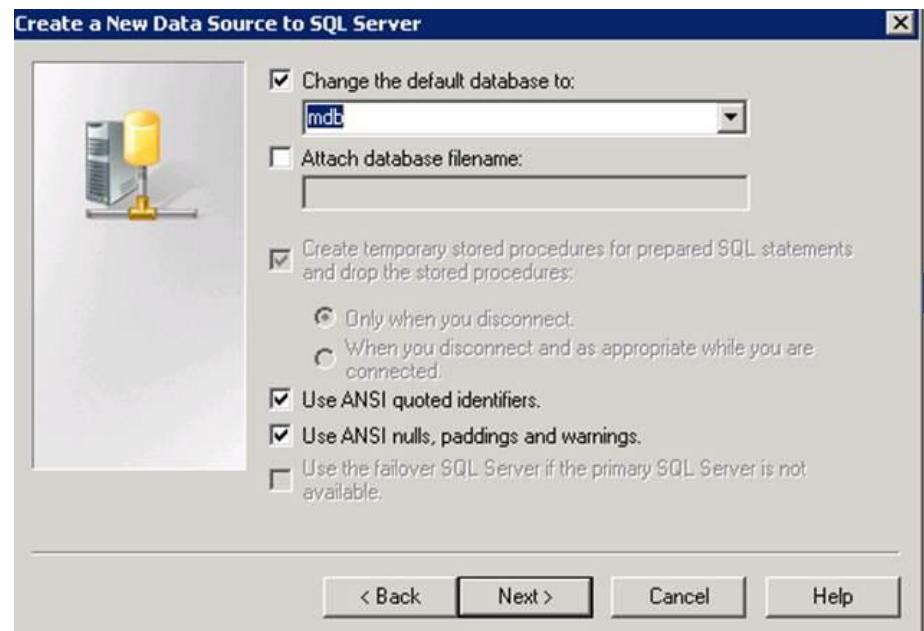
The Create a New Data Source to SQL Server page opens.



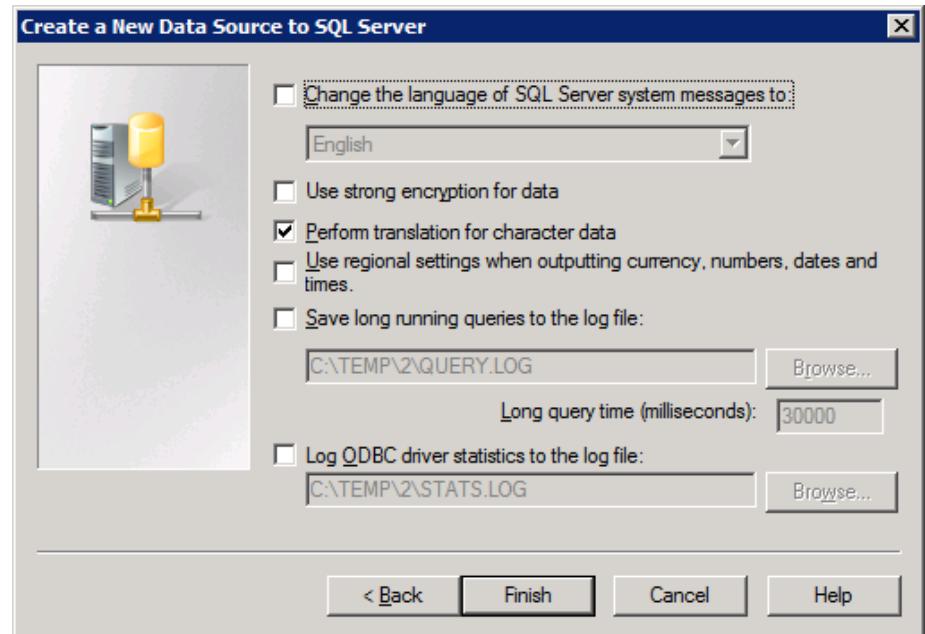
6. Select the With SQL Server authentication using a login ID and password from the user option.
7. Select the Connect to SQL Server and obtain default settings for the additional configuration options.

8. Type a Login ID and Password with access to the BOXI database, and click Next.

The Microsoft SQL Server DSN Configuration page opens.

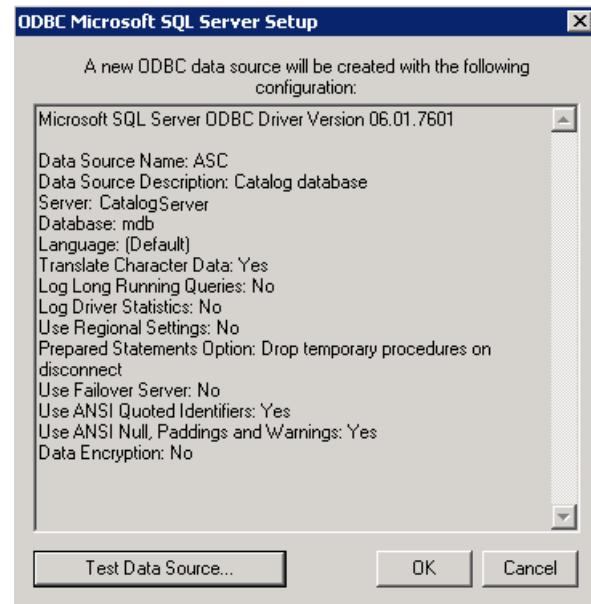


9. Select the Change the default database to check box and select the database name from the drop-down menu.
10. Click Next.



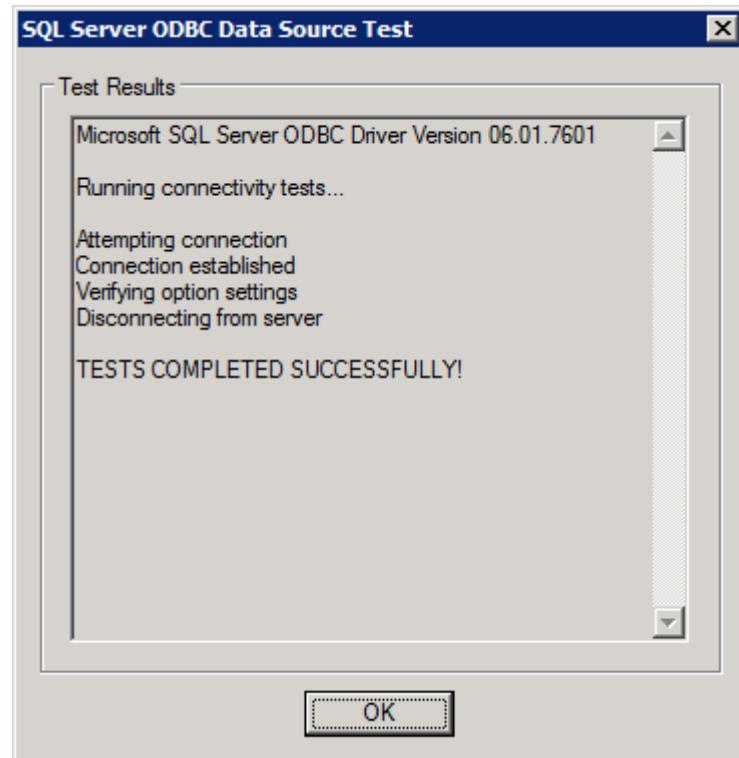
11. Click Finish.

The ODBC Microsoft SQL Server Setup page opens.



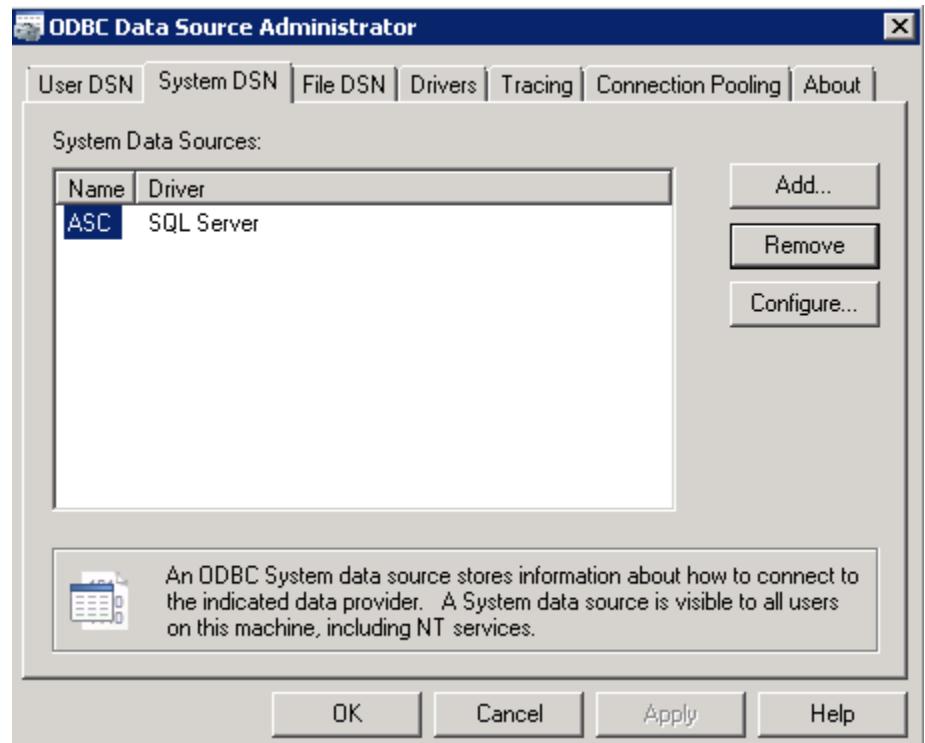
12. Click Test Data Source and verify the connection.

A confirmation message appears.



13. Click OK to close the message and click OK to close the ODBC Microsoft SQL Server Setup page.

The ODBC Data Source Administrator page opens.



14. Click OK.

Note: If the MDB Database used by CA Service Catalog and Software Delivery are created, a second ODBC Connection needs to be created to this MDB Database. This step is performed in the Post-Configuration section, but you could perform now if products are installed and the MDB Database is created.

The DSN and ODBC connection are complete.

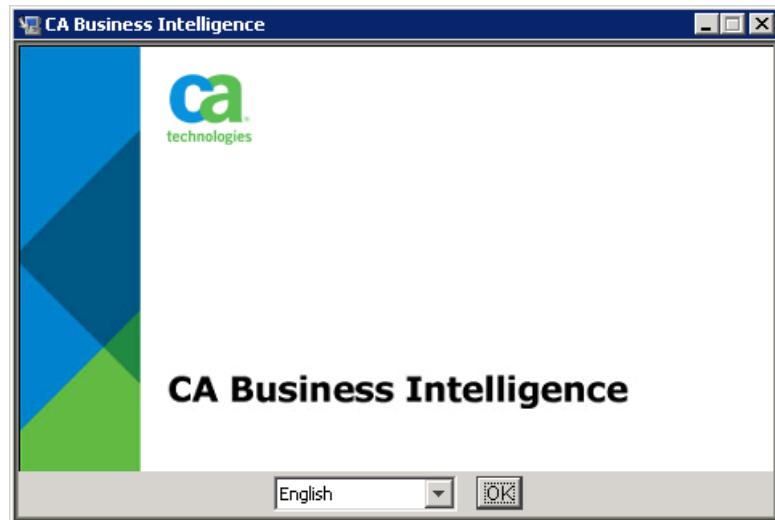
Install CA Business Intelligence

After you create the Microsoft SQL Database and configure the ODBC connection, install CA Business Intelligence. The installation is comprised of two installation wizards that must be executed sequentially.

Follow these steps:

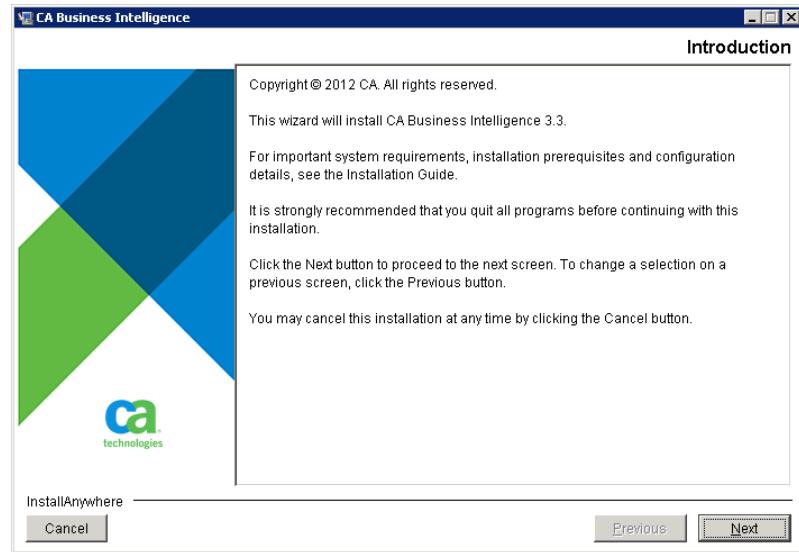
1. Open the CA Business Intelligence media.
2. Extract the CA Business Intelligence media to a folder on the server and open the media folder.
3. Right-click *cabiinstall.exe* and select Run as Administrator.

The CA Business Intelligence installation wizard opens.



4. Select your installation language and click OK.

The introduction page opens.



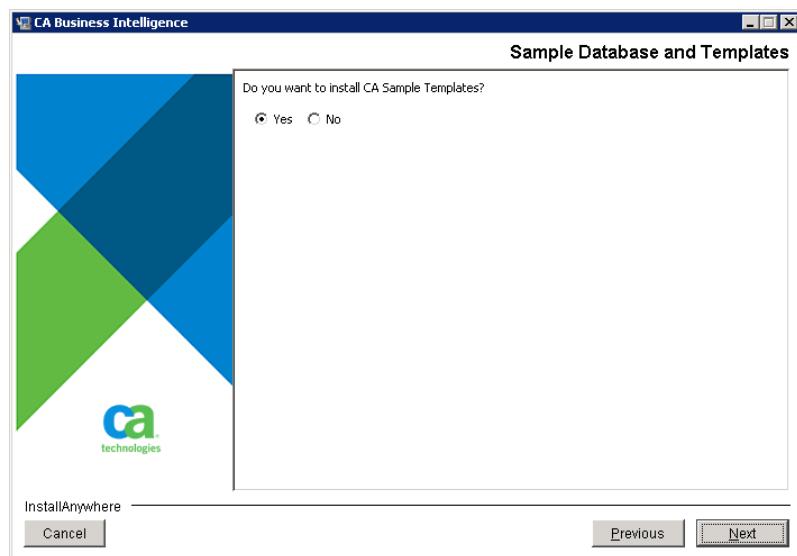
[Install CA Business Intelligence](#)

5. Click Next.

The License Agreement page opens.

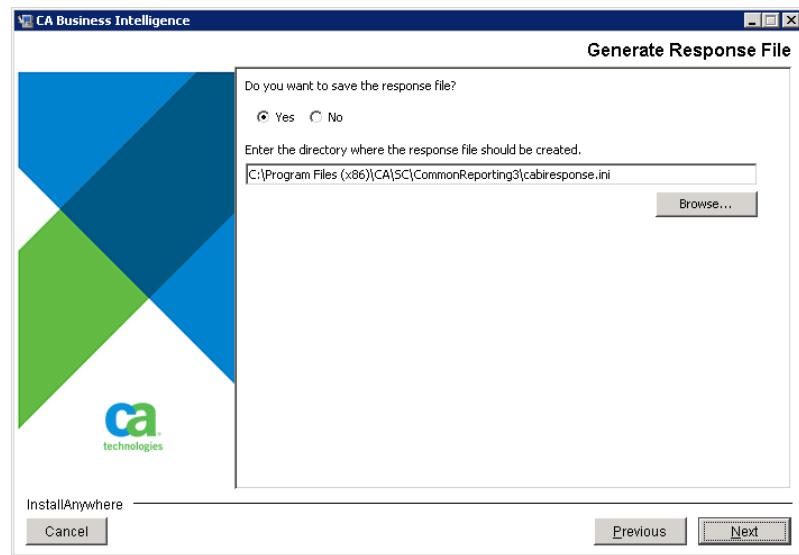
6. Scroll down the license text, select the I accept the License Accept option, and click Next.

The Sample Database and templates page opens. You can use the CA Sample templates for testing your CA Business Intelligence installation.



7. Verify that Yes is selected, and click Next.

The Generate Response File page opens. You can provide your installation settings to CA Support if necessary, using the response file.

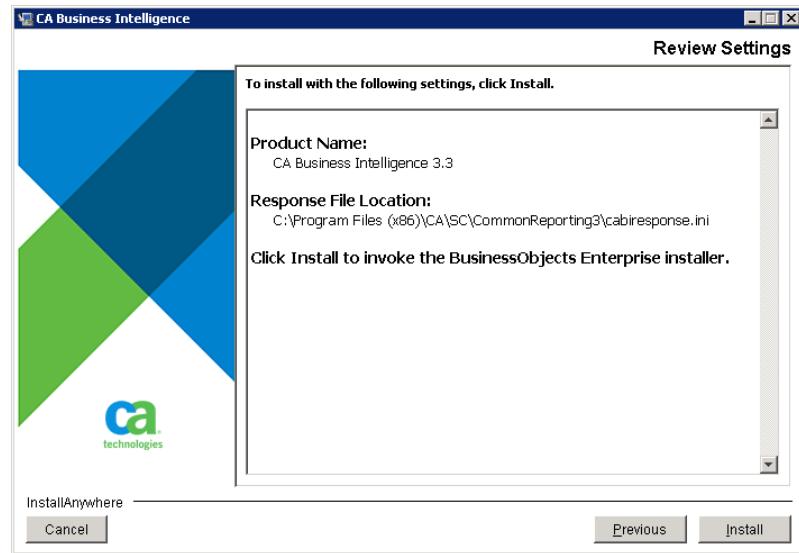


[Install CA Business Intelligence](#)

8. Verify Yes is selected.
9. Accept the location of the response file or click Browse to change the location of the response file and click Next.

Note: If you save the response file, you can provide your installation settings to CA Support if necessary.

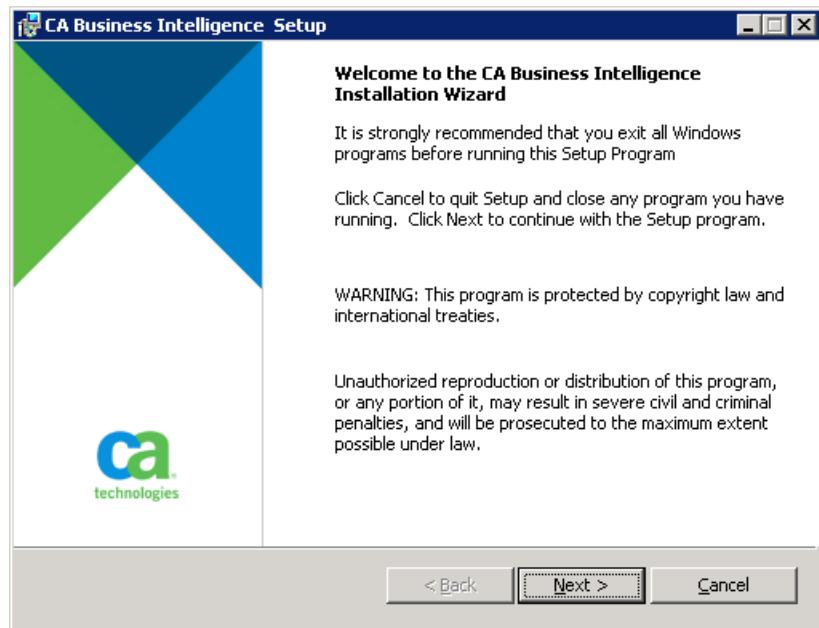
The Review Settings page opens.



10. Click Install.

The CA Business Intelligence Installation wizard opens.

Note: Verify the task bar as the CA Business Intelligence Setup wizard sometimes opens behind the CA Business Intelligence installation wizard.

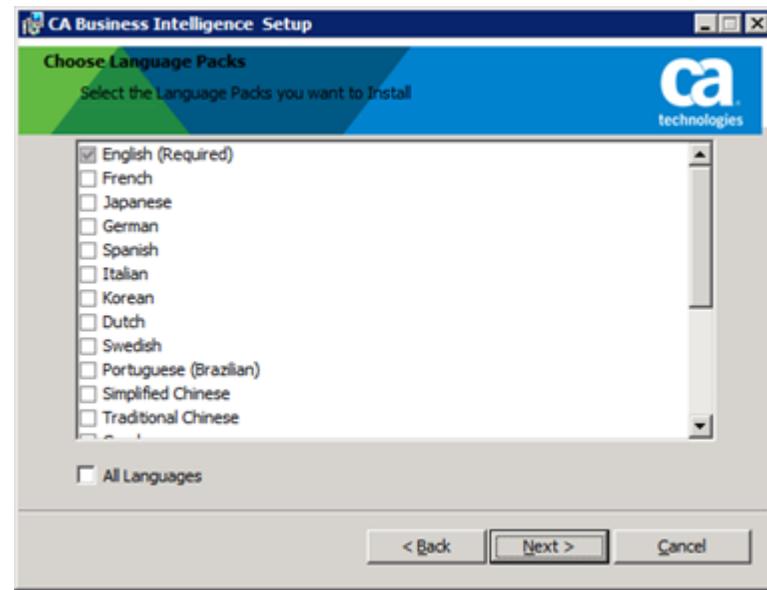


11. Click Next.

The License Agreement page opens.

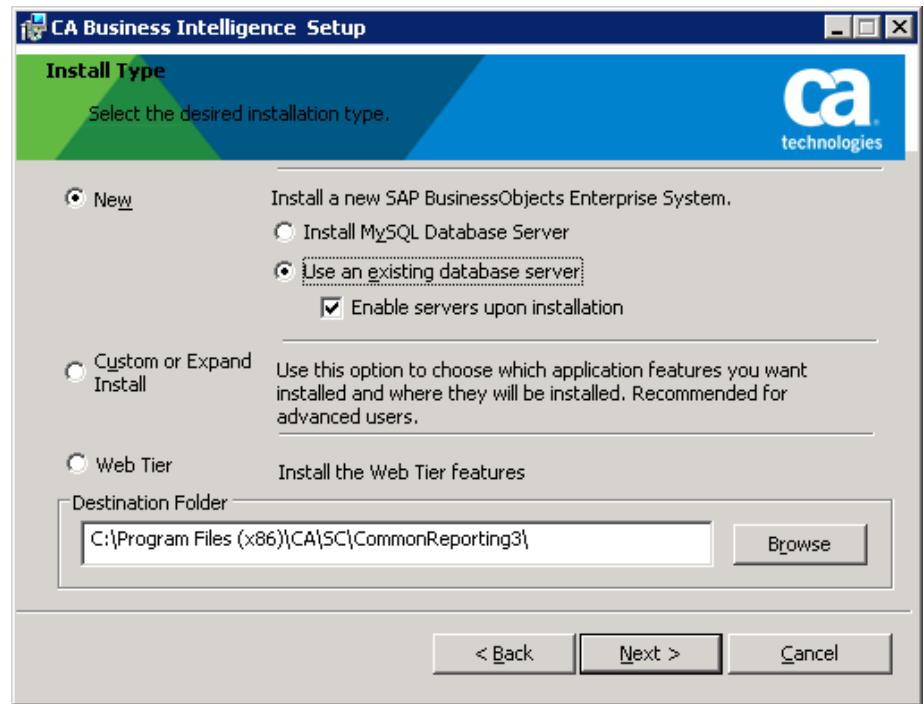
12. Select the I accept the License Agreement option and click Next.

The Choose Language Packs page opens.



13. Select the language packs you want to install and click Next.

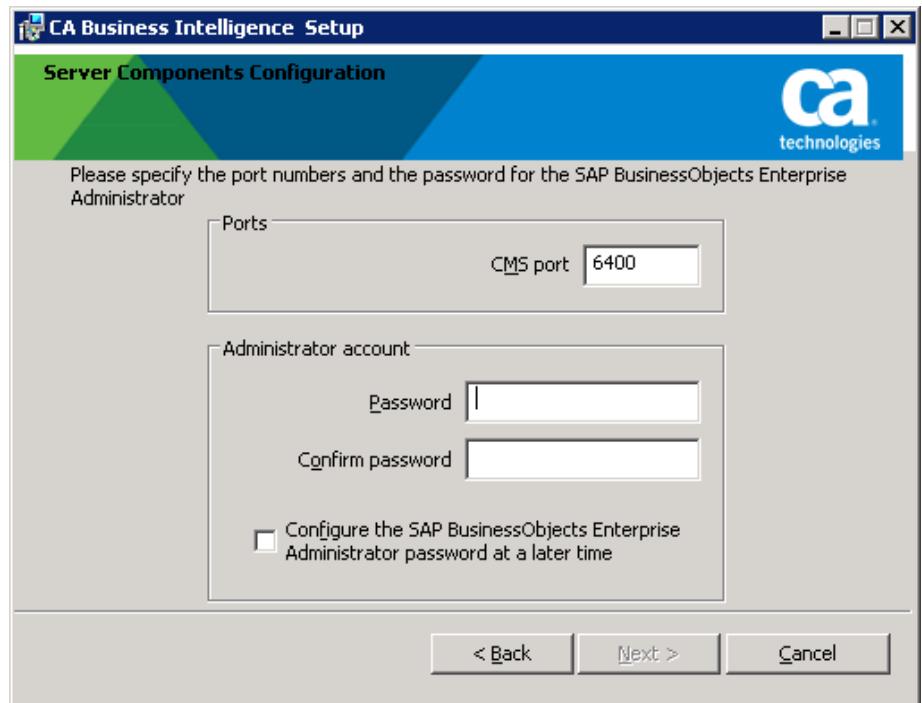
The Install Type page opens.



14. Complete the following details and click Next:

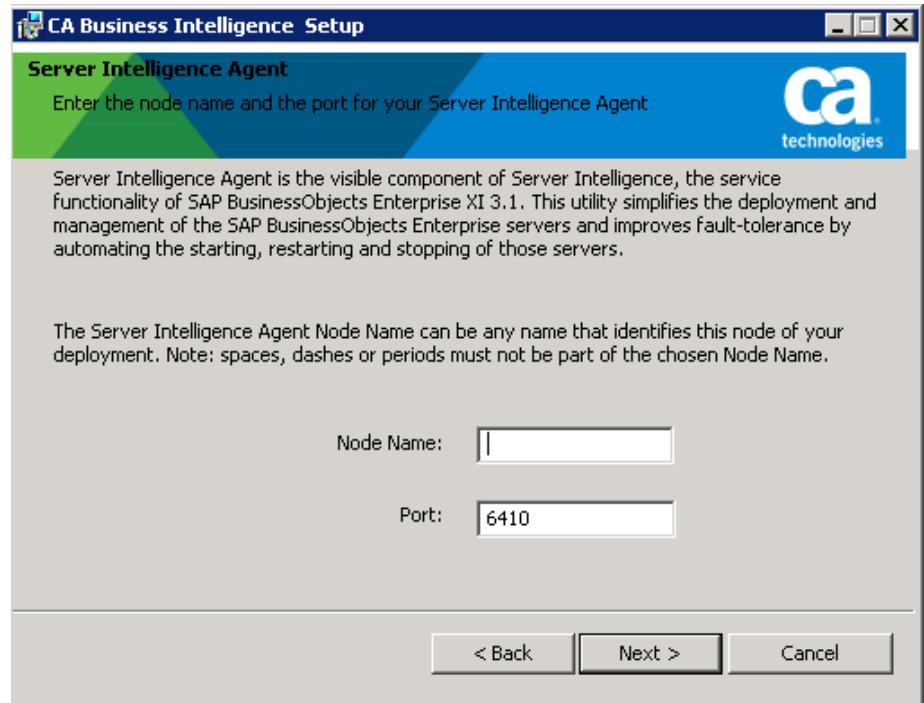
- a. Select New.
- b. Select Use an existing database server.
- c. Select the Enable servers upon installation check box.
- d. (Optional) Click Browse to select the Destination Folder.

The Server Components Configuration page opens.



15. Complete the following details and click Next:
 - a. Type the Port number (for example, 6400).
 - b. Type a password, confirm the password.
Note: Record the password in the [Installation Worksheet](#) (see page 19).
 - c. (Optional) Select *Configure the SAP BusinessObjects Enterprise Administrator at a later time* to set password later.
 - d. Click Next.

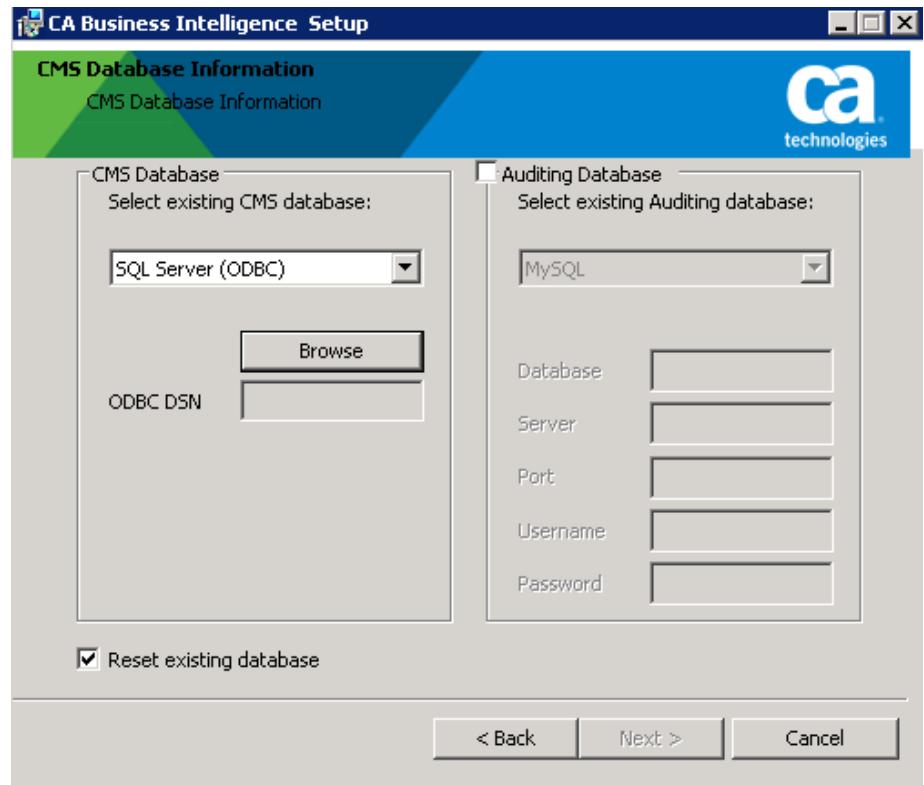
The Server Intelligence Agent page opens.



16. Type the Node Name (for example, Server name), Port (for example, 6410), and click Next.

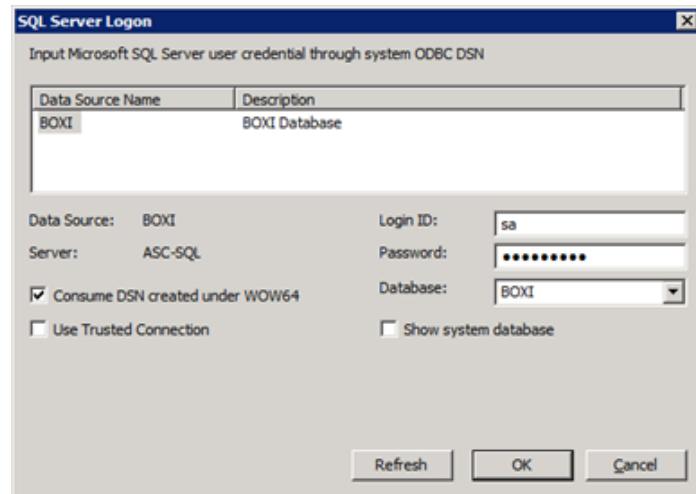
Default Node Name: localhost

The CMS Database Information page opens.



17. Select SQL Server (ODBC) from the drop-down list and click Browse to select CA Business Intelligence database.

The SQL Server Logon dialog opens.



18. Complete the following fields, and click OK:

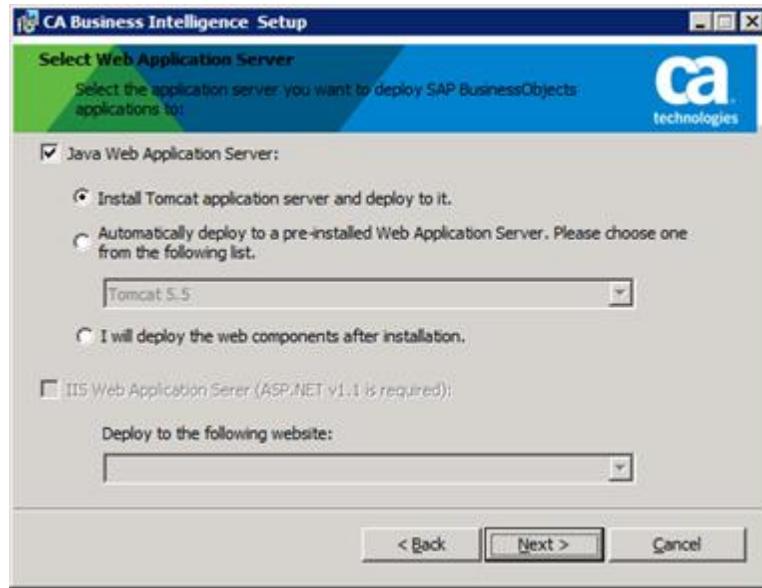
- Highlight the Data Source Name that is created earlier “BOXI”.
- Verify (sa) is the Login ID.
- Enter the Password for the Login ID.
- Select the Database “BOXI” for the drop-down list that was created for BOXI.
- Verify Consume DSN created under WOW64 is selected.

The CMS Database Information page opens.



19. Click Next.

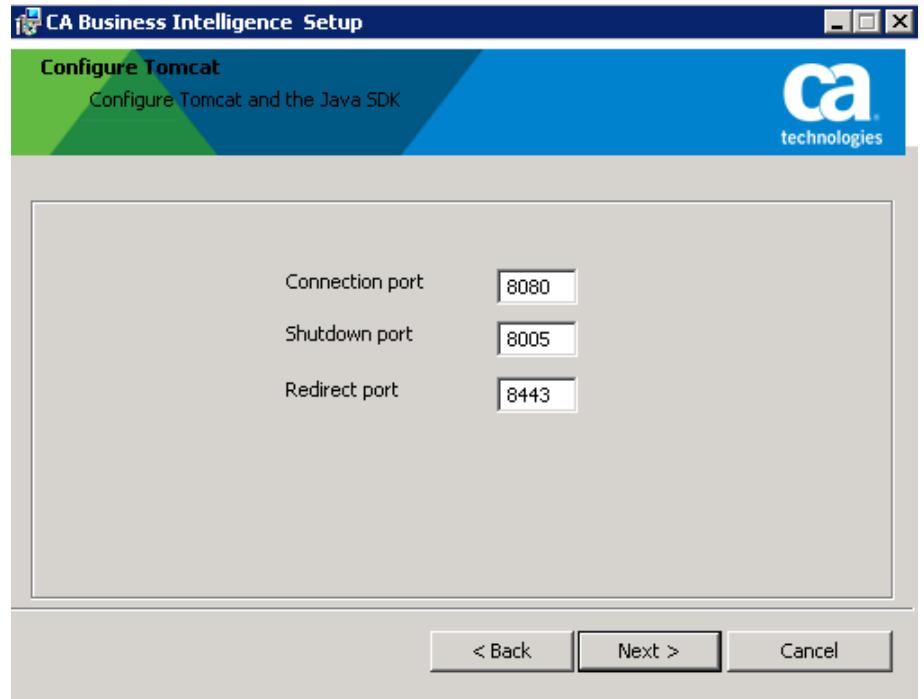
The Select Web Application Server page opens.



20. Verify the following settings and click Next:

- a. Verify that the Java Web Application Server check box is selected.
- b. Verify that the Install Tomcat application server and deploy to it option is selected.

The Configure Tomcat page opens.



21. Enter the following parameters and click Next.

Note: If a port is in use by another service, change the port information accordingly.

Connection port

Specifies the port number for the connection.

Value: 8080

Shutdown port

Specifies the shutdown port number.

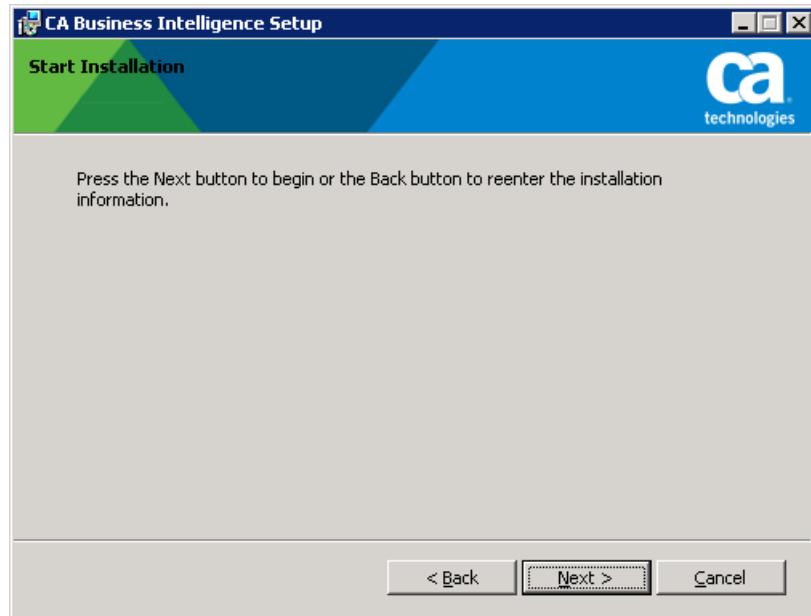
Value: 8005

Redirect port

Specifies the port number to redirect.

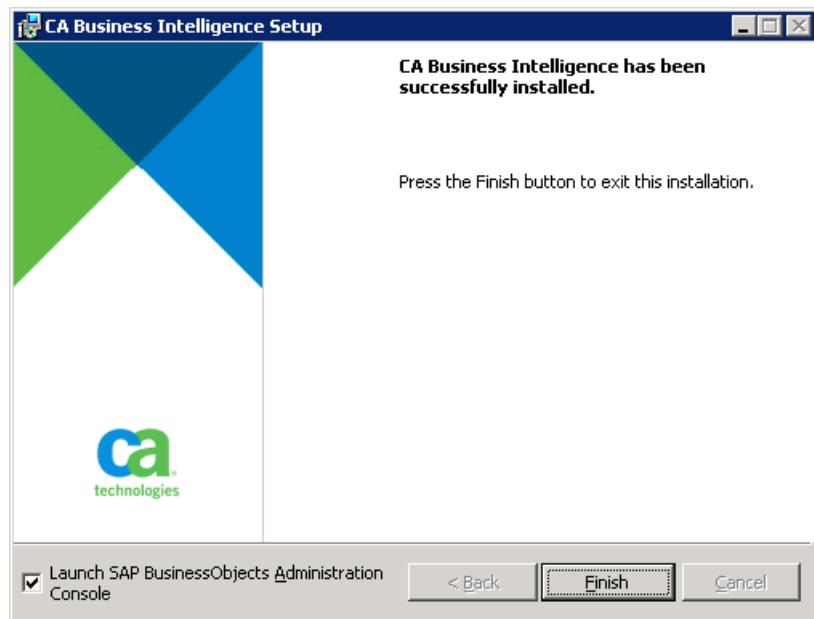
Value: 8443

The Start Installation page opens.

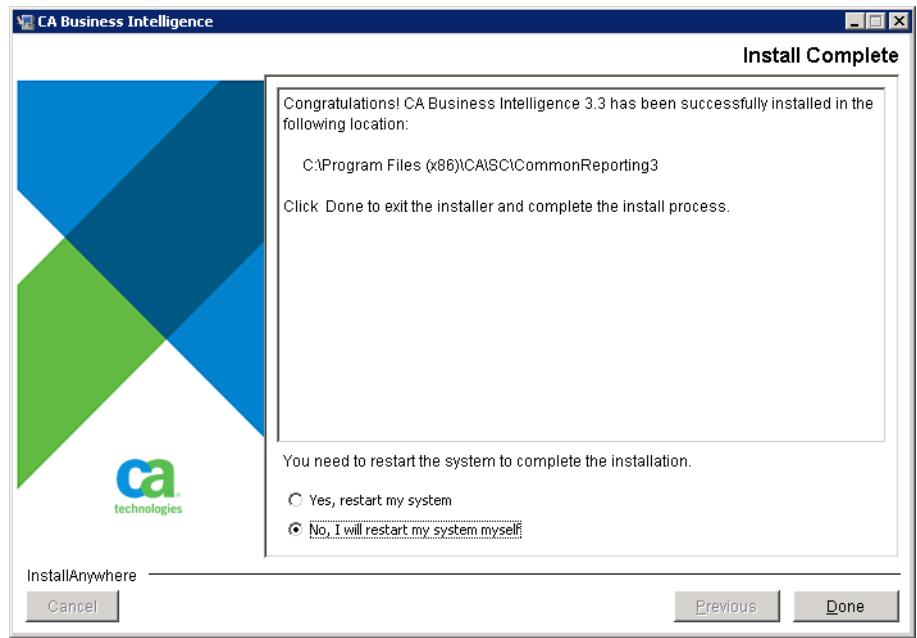


22. Click Next.

The installation begins. Installation process can take several minutes to complete.



The Install Complete page opens in the background.



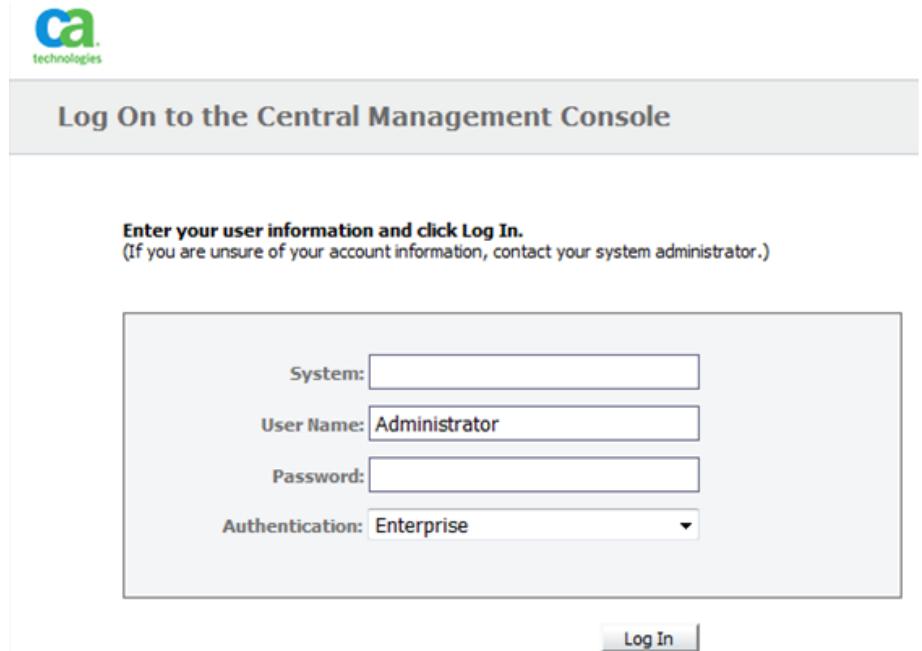
23. Select *No, I will restart my system myself* and click Done.

Note: In the background, the installation Complete page opens in the main installer. Complete the CA Business Intelligence configuration and then restart the server.

The main installer page closes and you can configure CA Business Intelligence using the second installation wizard.

24. Select the *Launch SAP BusinessObjects Administration Console* check box and click Finish.

The Central Management Console login page opens.



The image shows the 'Log On to the Central Management Console' page. At the top, the CA technologies logo is visible. Below it, a header bar contains the text 'Log On to the Central Management Console'. The main area contains instructions: 'Enter your user information and click Log In.' followed by '(If you are unsure of your account information, contact your system administrator.)'. Below these instructions is a form with four fields: 'System' (input field), 'User Name' (input field containing 'Administrator'), 'Password' (input field), and 'Authentication' (dropdown menu set to 'Enterprise'). At the bottom right of the form is a 'Log In' button.

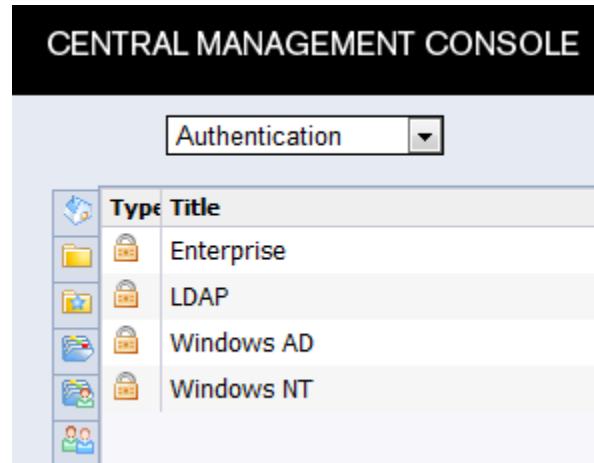
25. Complete the following details:

- a. Log in as Administrator.

Note: The password is the same as you provided during the installation. Refer the [Installation Worksheet](#) (see page 19) for the password.

- b. Select Enterprise in the Authentication drop-down menu.
- c. Click Log In.

The Central Management Console Home page opens.

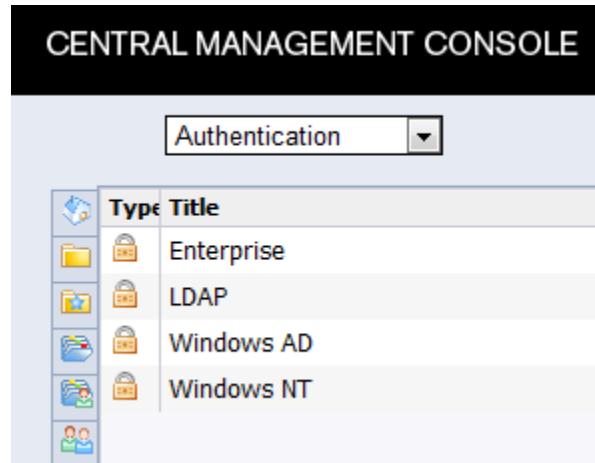


The screenshot shows the Central Management Console Home page. At the top, a black bar contains the text "CENTRAL MANAGEMENT CONSOLE". Below this, a dropdown menu is open, showing the text "Authentication" with a dropdown arrow. Below the dropdown is a table with the following data:

Type	Title
File	Enterprise
File	LDAP
File	Windows AD
File	Windows NT
File	Windows NT

26. Select Authentication from the drop-down.

The Authentication page opens displaying a list of authentication options.

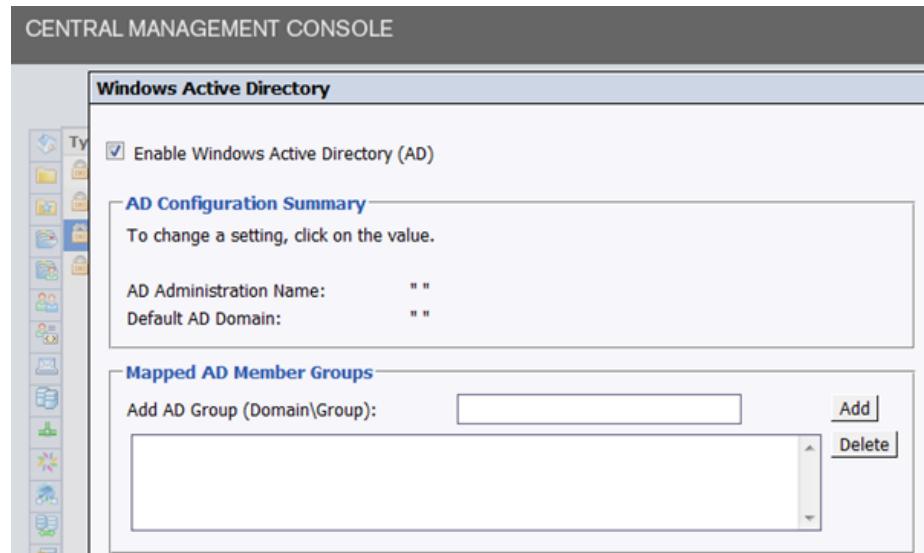


The screenshot shows the 'CENTRAL MANAGEMENT CONSOLE' window. A dropdown menu is open, showing the option 'Authentication'. Below the menu, a table lists four authentication types: 'Enterprise', 'LDAP', 'Windows AD', and 'Windows NT'. Each entry has a small icon to its left.

Type	Title
Enterprise	
LDAP	
Windows AD	
Windows NT	

27. Double-click Windows AD.

The Windows AD settings page opens.



The screenshot shows the 'CENTRAL MANAGEMENT CONSOLE' window with the 'Windows Active Directory' settings page open. The left sidebar shows a list of icons. The main area has a title 'Windows Active Directory'. Under this, there is a section with a checked checkbox for 'Enable Windows Active Directory (AD)'. Below this is a 'AD Configuration Summary' section with two entries: 'AD Administration Name: " "' and 'Default AD Domain: " "'.

Windows Active Directory

Enable Windows Active Directory (AD)

AD Configuration Summary

To change a setting, click on the value.

AD Administration Name: " "
Default AD Domain: " "

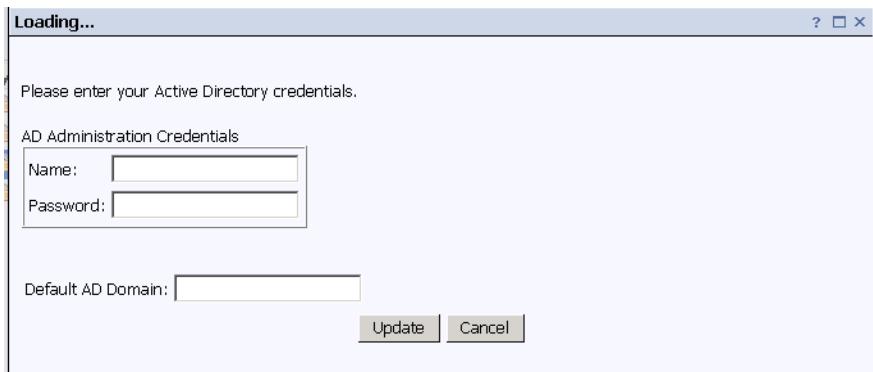
Mapped AD Member Groups

Add AD Group (Domain\Group): Add Delete

28. Complete the following details:

- a. Select the Enable Windows Active Directory (AD) check box.
- b. Click the double quotes “ “ next to configure the AD Administrator Name.

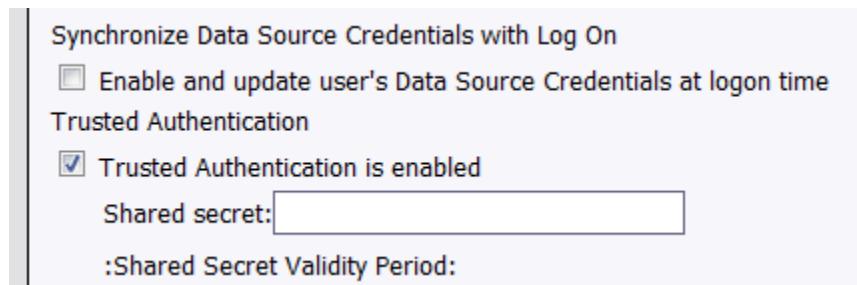
The Windows Active Directory page opens.



- c. Enter your Active Directory credentials.
- d. Click Update.
- e. Close the Windows AD configuration window.

29. Double-click Enterprise.

The Enterprise settings page opens.



30. Complete the following details:
 - a. Select the Trusted Authentication is enabled check box.
 - b. Enter a string in the Shared secret field. Update this value in the [Installation Worksheet](#) (see page 19), CA Business Intelligence section.
 - c. Click Update.
 - d. Click Log Out and close the window.
31. Restart the server.

You have installed CA Business Intelligence.

Verify Installation

Log in to InfoView and verify that the component is installed.

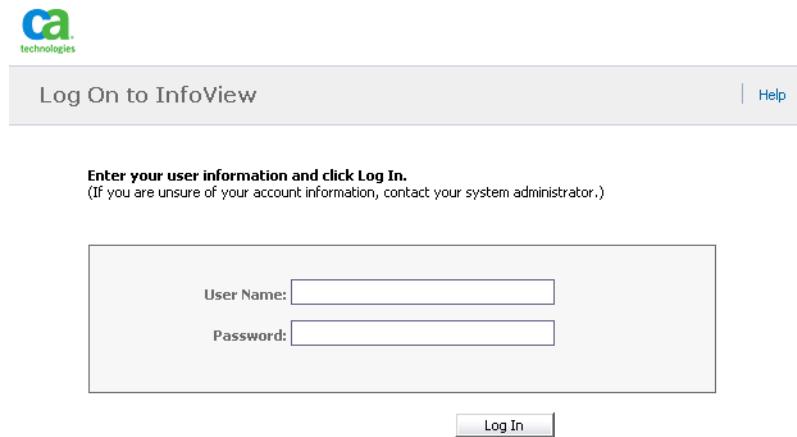
Follow these steps:

1. Log in to the BusinessObject Enterprise Java InfoView server as an administrator.

2. Do one of the following tasks:

- Select Start, All Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, BusinessObjectsEnterprise Java InfoView
- Type `http://<CABI_Server>:<Port_Number>/InfoViewApp`, in a browser and press Enter.

The Log On to InfoView page opens.



The screenshot shows the 'Log On to InfoView' page. At the top, there is a CA technologies logo. To the right of the logo is a 'Help' link. The main title 'Log On to InfoView' is centered above a large input field. Inside this field, there is a message: 'Enter your user information and click Log In. (If you are unsure of your account information, contact your system administrator.)'. Below this message are two input boxes: one for 'User Name' and one for 'Password'. At the bottom right of the input field is a 'Log In' button.

3. Log in to CA Business Intelligence as Administrator (Default Username: Administrator).

If you can log in and access CA Business Intelligence InfoView page, the installation was successful.

Install CA Process Automation

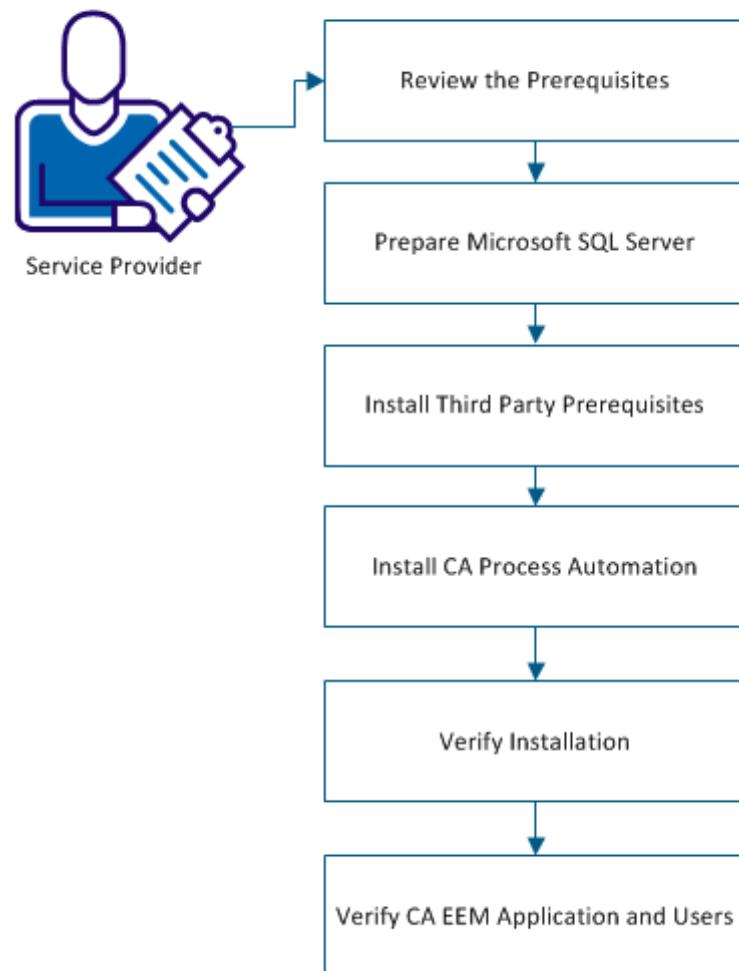
The CA Process Automation component of CA Automation Suite for Clouds automates work flows and processes within an organization.

The CA Process Automation r4.2 SP1 installation requires two ISO images:

- The CA Process Automation r4.2 SP1 Third Party Prerequisites – DVD 1 is used to install third-party prerequisites (JBoss, Hibernate, JDBC Jar, and TAPI Jar). Install the prerequisite software from the installation ISO. Do not use preexisting versions that are already installed on your system.
- **Note:** The CA Process Automation installation depends on certain third-party components being present on the server. Install all the necessary third-party requirements before installing the CA Process Automation software. The third-party prerequisites require at least 8 GB of disk space.
- The CA Process Automation r4.2 SP1 Product Installation – DVD 2 is used to install the CA Process Automation component.

This scenario describes how to install the CA Process Automation component for the CA Automation Suite for Clouds solution.

Install CA Process Automation



Follow these steps:

1. [Review the Prerequisites](#) (see page 76).
2. [Prepare Microsoft SQL Server](#) (see page 77).
3. [Install Third-Party Prerequisites](#) (see page 78).
4. [Install CA Process Automation](#) (see page 85).
5. [Verify Installation](#) (see page 105).
6. [Verify CA EEM Application and Users](#) (see page 106).

Review the Prerequisites

Refer to the Review System and Hardware Requirements section for general installation requirements. Complete and verify the following requirements before you begin the installation:

- Install Java JDK Version 1.7 or above (64 bit).
- [Prepare Microsoft SQL Server](#) (see page 77).

Prepare Microsoft SQL Server

The Microsoft SQL Server must fulfill the prerequisites for installing CA Process Automation.

- The SQL Server must be installed or configured with the mixed mode authentication. You can specify an account with the SQL Server authentication during the Orchestrator installation.
- The Orchestrator installer requires user credentials with Administrator privileges to create the CA Process Automation databases.
- The SQL Server collation for CA Process Automation databases must be SQL_Latin1_General_CI_AS. By default, the CA Process Automation installer creates databases with this collation.

Follow these steps:

1. Navigate to the ConfigurationFile.ini file, which is created in a path similar to the following text:
`C:\ Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\yyyymmdd_hhmmss`
2. Verify that the security mode setting resembles the following text:
The default is Windows Authentication. Use "SQL" for Mixed Mode Authentication.
`SECURITYMODE="SQL"`
3. Verify that the setting for the SQL system administrator account credentials resembles the following text:
; Windows account(s) to provision as SQL Server system administrators.
`SQLSYSADMINACCOUNTS="hostname\Administrator"`
4. Verify that the setting for collation resembles the following text:
; Specifies a Windows collation or an SQL collation to use for the Database Engine.
`SQLCOLLATION="SQL_Latin1_General_CI_AS"`

Install Third-Party Prerequisites

Perform these steps on the machine where you intend to install CA Process Automation:

Important! The CA Process Automation installation depends on certain third-party components being present on the server. Install all the necessary third-party requirements before installing the CA Process Automation software.

Note: Ensure Java Runtime Environment-64 bit is installed.

Follow these steps:

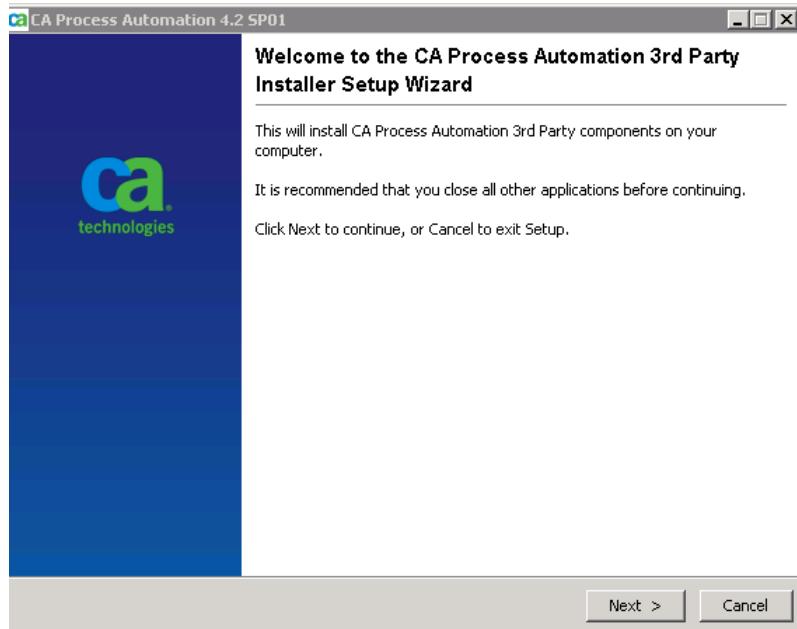
1. Open the *CA Process Automation r4.2 SP1 Third Party Prerequisites – DVD 1* media and run the *Third_Party_Installer_Windows.exe*.

The file initiates the installation and prompts you to select a language.

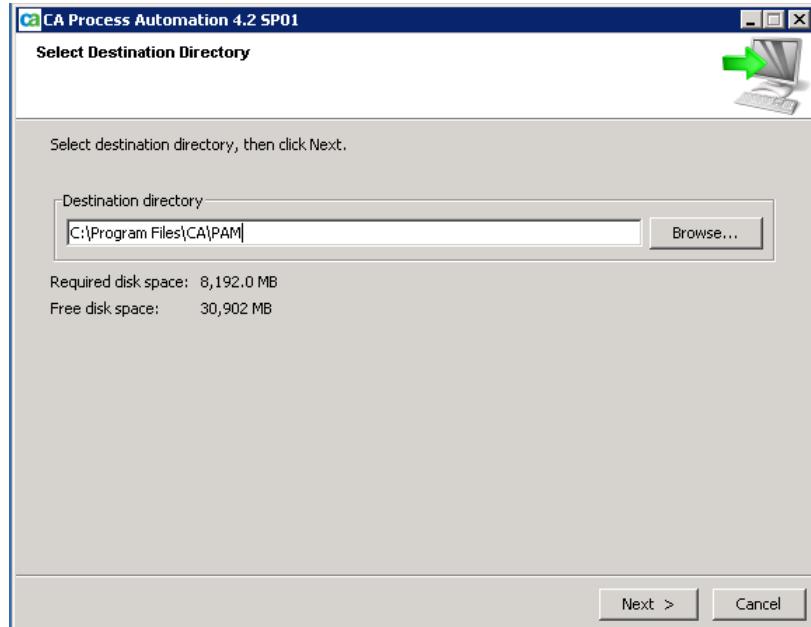


2. Select English from the drop-down list, and click OK.

The Welcome window opens.



3. Click Next on the Welcome window to continue.
The License Agreement window opens.
4. Select I accept the terms of the License Agreement, and click Next.
The Destination Directory window opens.

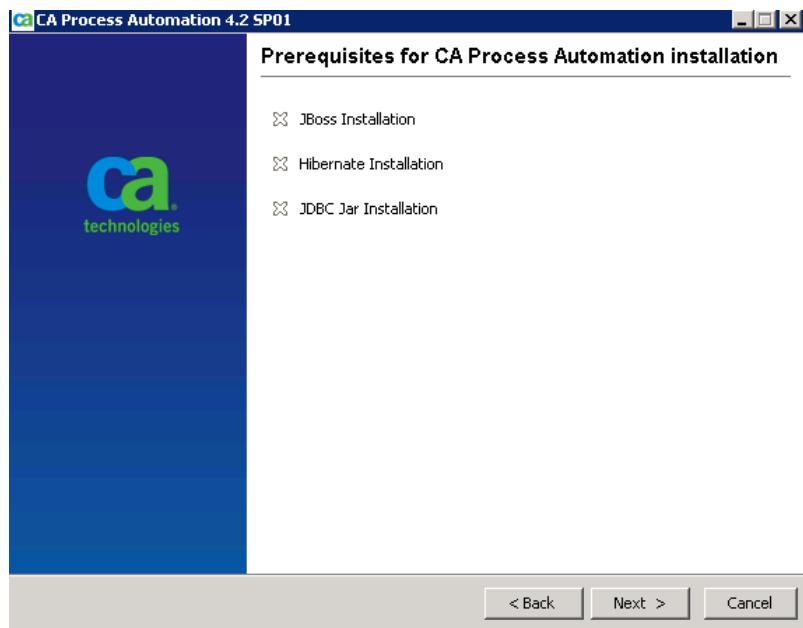


5. Accept the default Destination Directory or Specify the Destination Directory for installing CA Process Automation and click Next.

Note: The length of the path name for the destination directory must not exceed 255 characters. The best practice is to keep the field length to fewer than 64 characters.

The installer creates the folder automatically.

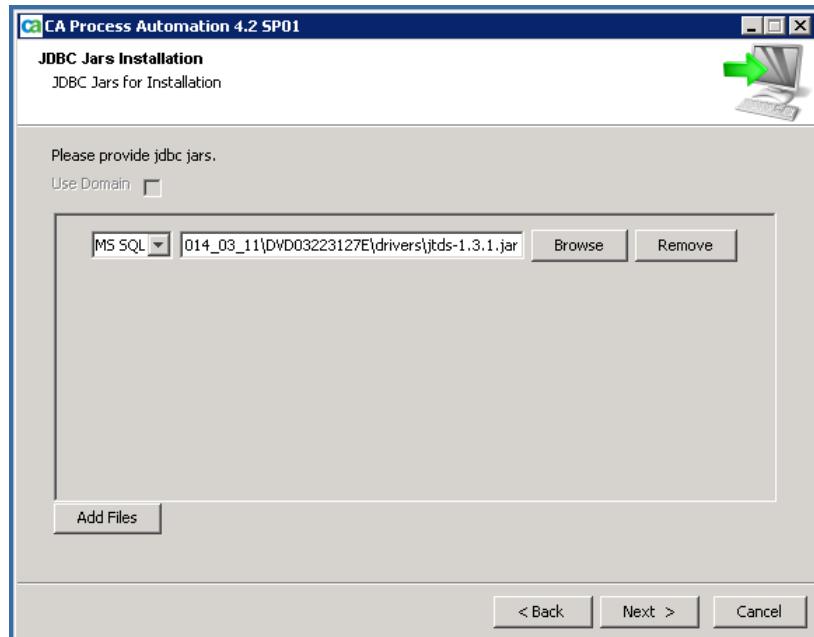
The Prerequisites for CA Process Automation Installation window opens.



6. Click Next.

Monitor the installation of JBoss and third-party components.

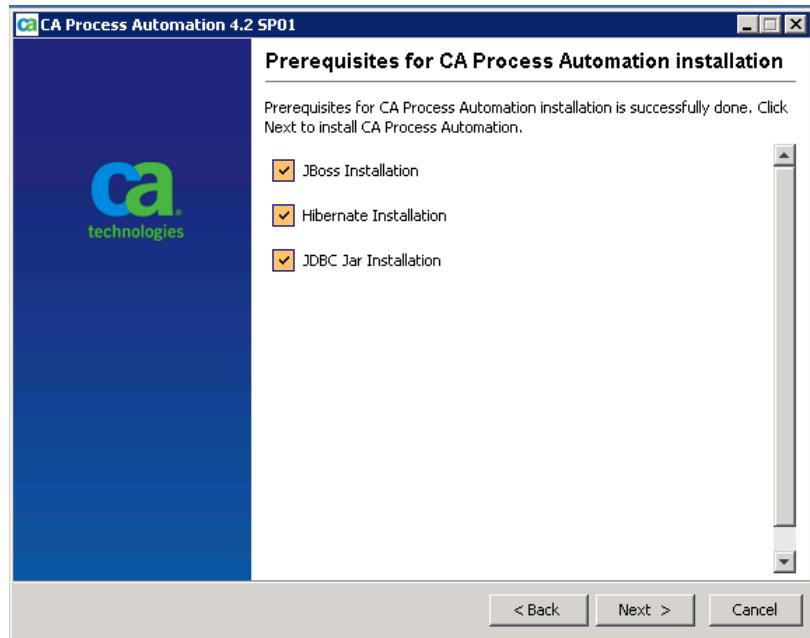
The JDBC Jars Installation window opens.



7. Click Add Files and select MS SQL from the drop-down list to accept the default jdbc.jar path and click Next.

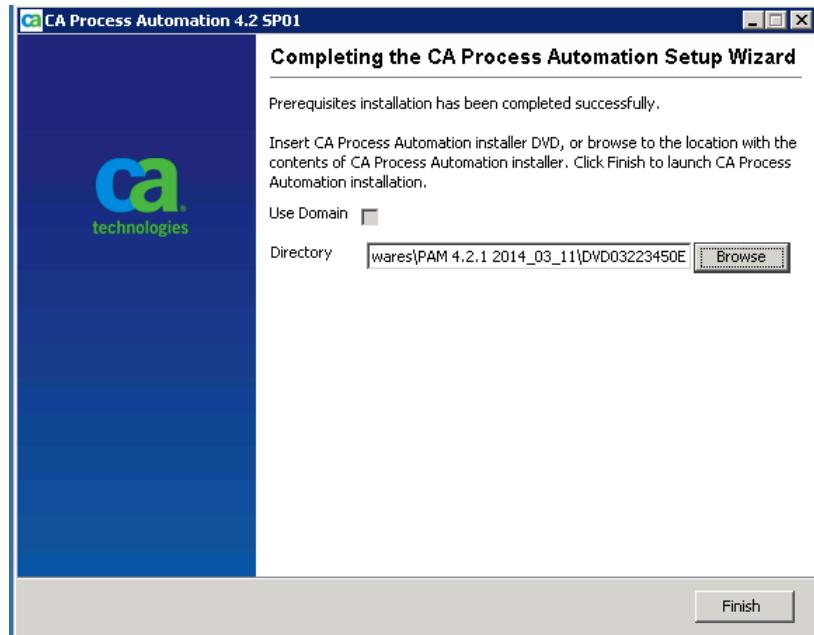
Note: Do not change the jdbc jar path (The Installation Wizard defaults to the correct location).

The *Prerequisites for CA Process Automation installation* window opens.



8. Click Next to progress to the CA Process Automation Setup Wizard.

The Completing CA Process Automation Setup Wizard opens.



9. Change the directory to CA Process Automation r4.2 SP1 Product Installation – DVD 2 to install CA Process Automation and click Finish.

Note: The CA Process Automation installer takes several minutes to appear.

The third-party prerequisites are installed and the CA Process Automation Installation window opens.

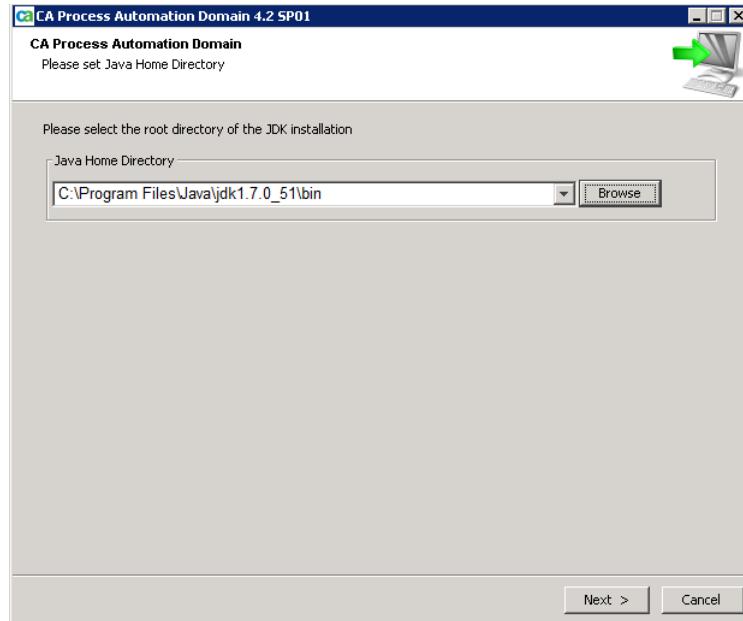
Install CA Process Automation

After you install the third-party prerequisites, install the CA Process Automation component.

Follow these steps:

1. Click Next on the CA Process Automation installation window.
The License Agreement window opens.
2. Read the License Agreement, select the I accept the terms of the License Agreement option, and click Next.

The Java Home Directory window opens.

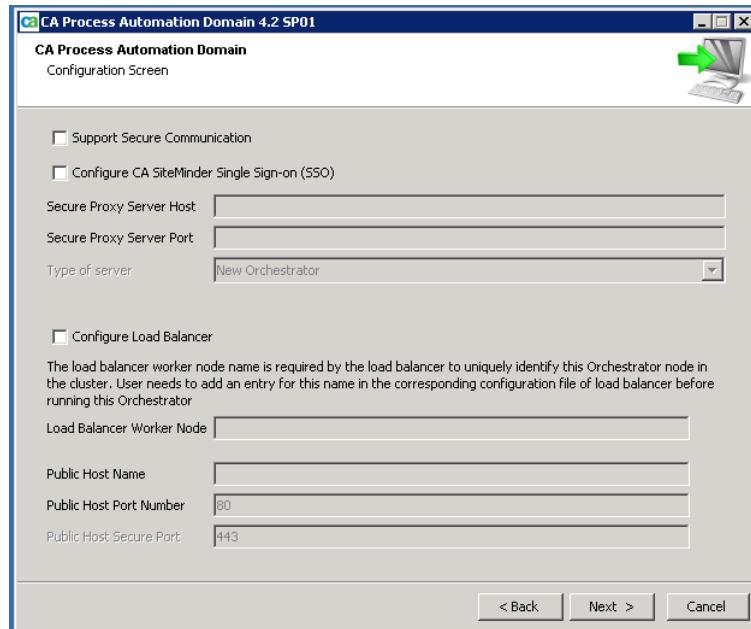


3. Specify the file path of the Java Home Directory, or click Browse and navigate to the directory path, then click Next.

The installation begins.

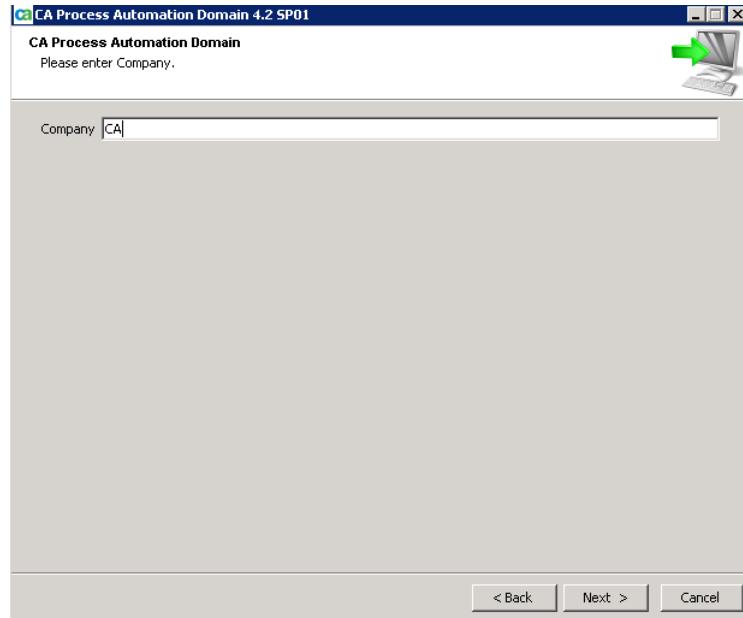
Note: The files take several minutes to copy.

The CA Process Automation Domain Configuration window opens.



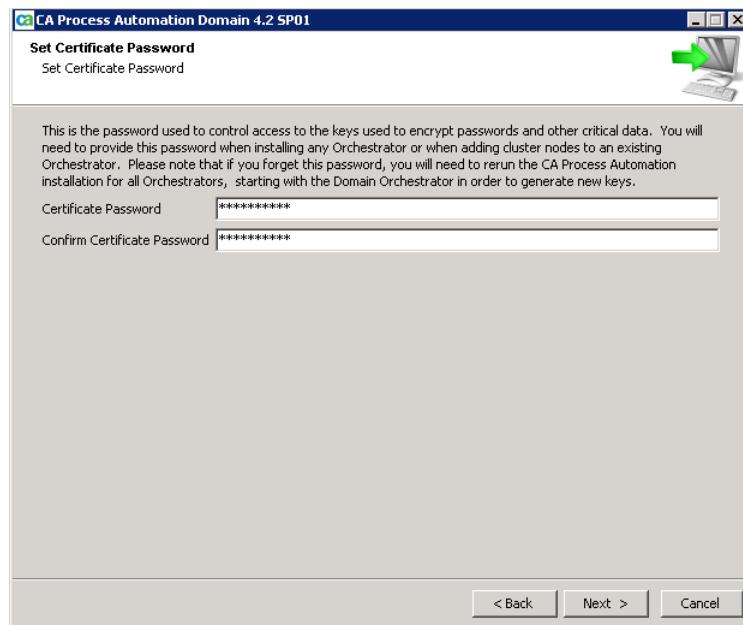
4. Verify that the Configure Single Sign-on and Configure Load Balancer check boxes are cleared. This functionality is not needed in CA Automation Suite for Clouds. Click Next.

The Please enter company window opens.



5. Type your company name, and click Next.

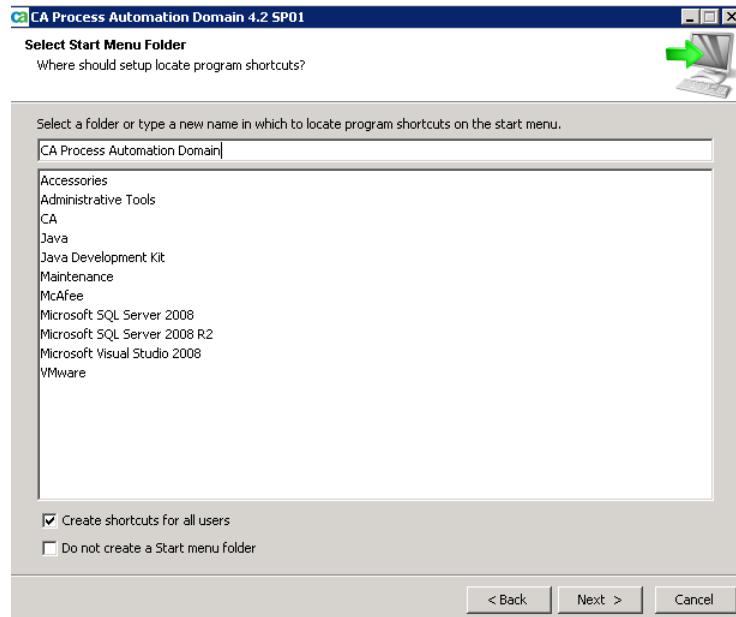
The Set Certification Password window opens.



6. Type the Certificate Password twice, and click Next.

Important! This password controls access to the keys used to encrypt passwords and other critical data. Record this password on the [Installation Worksheet](#) (see page 19) to refer during the installation.

The Select Start Menu Folder window opens.



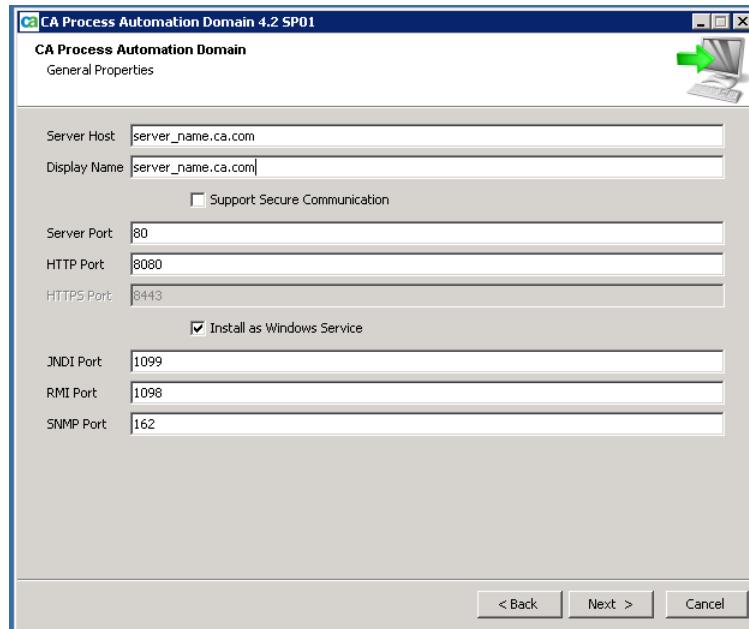
7. Create a folder named CA Process Automation Domain.

- Select the **Create shortcuts for all users** check box.
- Ensure **Do not create a Start menu folder** check box is cleared.

These options create a folder that stores program shortcuts and is accessible from the Start Menu.

8. Click Next.

The General Properties window opens.



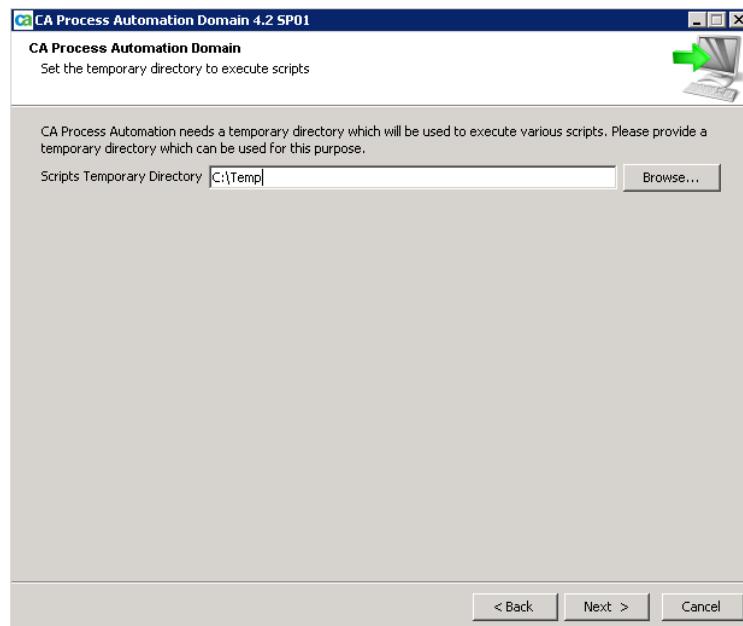
9. Type the General Properties for the CA Process Automation domain. Use the appropriate default values that are found on the CA Automation Suite for Clouds Solution Worksheet.

Note: CA Process Automation and CA Service Catalog both use HTTP Port 8080 by default. If installed on the same server, change one of the port numbers to avoid a conflict.

- a. Ensure that the Support Secure Communication check box is cleared, selecting this option changes the port number.
- b. Select Install as Windows Service.

10. Click Next.

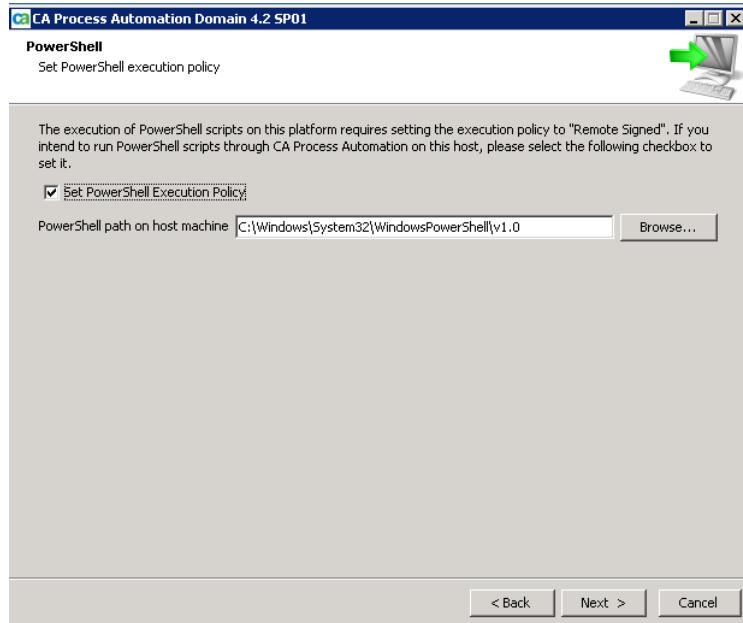
The Set the temporary directory to execute scripts window opens.



11. Set the Scripts Temporary Directory to C:\TEMP, and click Next.

Note: The preferred directory is \TEMP. All users must have the permission to access this directory.

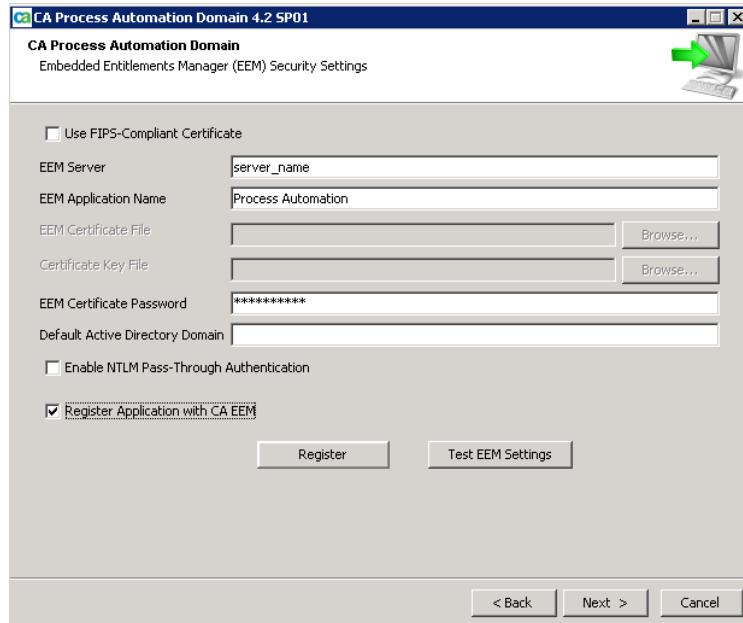
The Set Powershell execution Policy window opens.



12. Select the Set PowerShell Execution Policy check box.
13. Accept the default path (C:\Windows\System32\WindowsPowerShell\v1.0) to the PowerShell.exe, and click Next.

PowerShell scripts are enabled on the system.

The CA EEM Security Settings window opens.



14. Specify the directory server properties for CA EEM and register the CA Process Automation component to the CA EEM server. Use the appropriate values that are found on the [Installation Worksheet](#) (see page 19).

Note: Do not enter any values to the *EEM Certificate File* and the *Certificate Key File* fields because the solution does not use them.

- a. Verify that FIPS-compliant Certificate is cleared.
Data that is transferred between the CA Process Automation and CA EEM servers is encrypted using the MD5 algorithm.
- b. Type the fully qualified CA EEM server name.
- c. Verify that the CA EEM Application Name is Process Automation.
- d. Type the CA EEM Certificate Password.
- e. Ensure that the Enable NNTLM Pass-Through Authentication check box is cleared.
- f. Select Register Application with CA EEM.
- g. Click Register.

The EEM Credentials window opens.

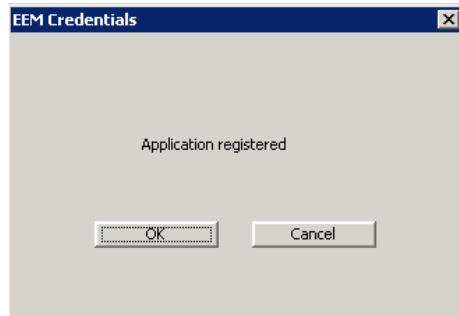


h. Type EiamAdmin for the CA EEM Administrator Username

and password for the EiamAdmin user.

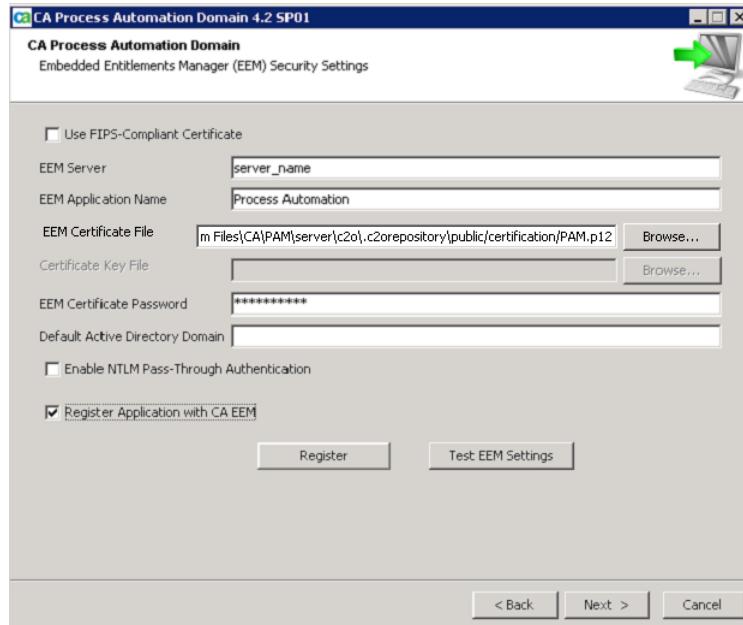
i. Click OK.

CA Process Automation is registered to the CA EEM server. A confirmation window opens stating that the application is registered.



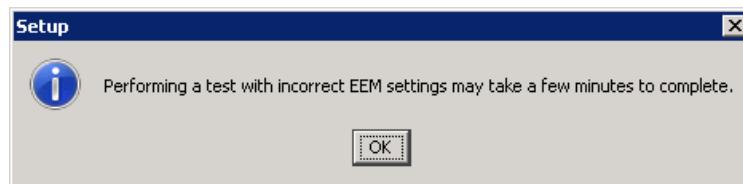
15. Click OK to return to the CA EEM Security Settings window.

On the CA EEM Security Settings window, verify that the CA EEM Certificate File field is populated with the location of the PAM.p12 file.



16. Click the Test EEM Settings to test CA Process Automation administrator settings that are defined in the CA EEM directory.

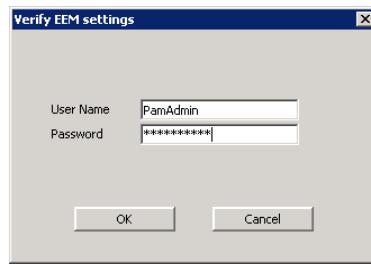
A message appears.



Note: The authentication fails if the appropriate users were not added during the CA EEM installation.

17. Click OK.

The Verify EEM Settings window opens.

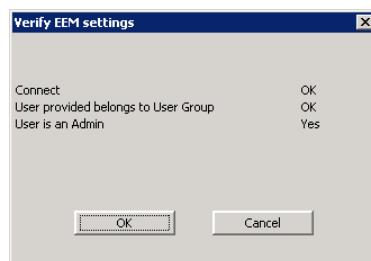


18. Type the default username of PAMAdmin, and the password that was created in the Install CA EEM section, and click OK.

The CA EEM settings for the PAMAdmin are authenticated in the CA EEM directory.

19. Verify the CA EEM settings for the PAMAdmin. The status must appear as follows:

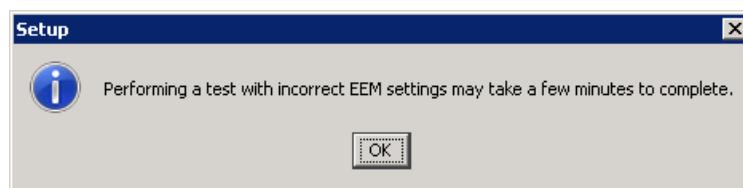
- Connect: OK
- User provided belongs to User Group: OK
- User is an Admin: Yes



20. Click OK.

21. Click the Test EEM Settings to test CA Process Automation user settings that are defined in the CA EEM directory.

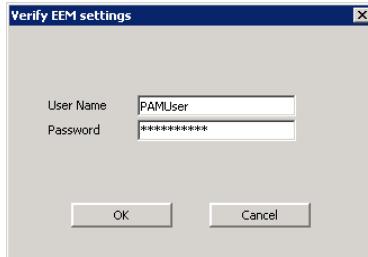
A message appears.



Note: The authentication fails if the appropriate users were not added during the CA EEM installation.

22. Click OK.

The Verify EEM Settings window opens.

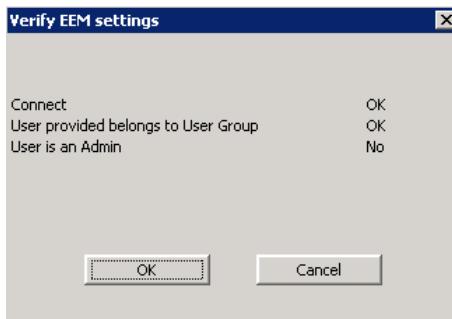


23. Type the username for PAMUser and the password that was created in the Install CA EEM section, and click OK.

The CA EEM settings for PAMUser are authenticated in the CA EEM directory.

24. Verify the CA EEM settings for the PAMUser. The status must appear as follows:

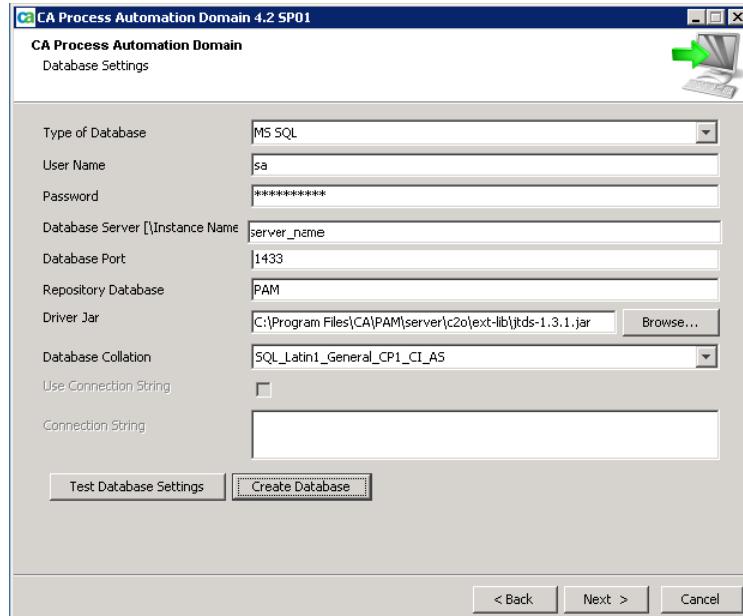
- Connect: OK
- User provided belongs to User Group: OK
- User is an Admin: No



25. Click OK when settings are displayed.

26. Click Next after you have tested the CA Process Automation Administrator and Users on the CA EEM Security Settings window.

The Database Settings window opens.



27. Make the following changes, in the Database Settings to create a CA Process Automation database. Use the appropriate values that are found on the [Installation Worksheet](#) (see page 19).

- Change the Type of Database from the drop-down list to MS SQL.
- Type a User Name for a Microsoft SQL Administrator that can access the Microsoft SQL Server using the Microsoft SQL Authentication method.
- Type the Password for the Microsoft SQL Administrator user.
- Change the Database Server to the Microsoft SQL Server host name.
- Verify the Database Port of the Microsoft SQL Server host.
Note: If SQL is using a Named Instance, type the Dynamic TCP/IP Port.
- Verify that the Repository Database name is PAM.
- Verify that the Driver Jar location is set to the sqljdbc.jar file path.

- h. Verify that the Database Collation is set to SQL_Latin1_General_CI_AS.

- i. Click Create Database.

The CA Process Automation database is created and a confirmation message appears.

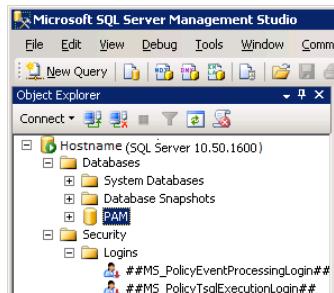
- j. Click OK.

28. (Optional) Verify that the PAM Database has been created successfully.

- a. Open Microsoft SQL Server Management Studio and expand Databases.

- b. Confirm that the PAM database has been created.

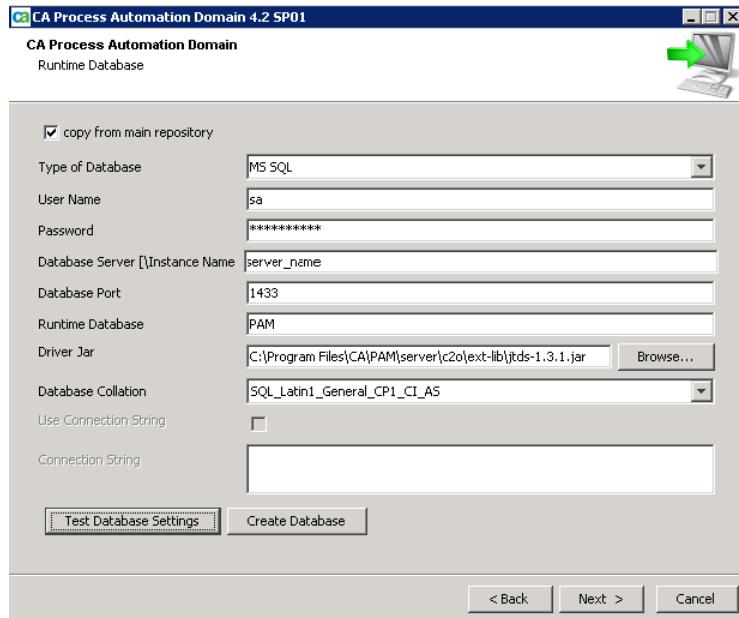
The PAM Database in MS SQL Server.



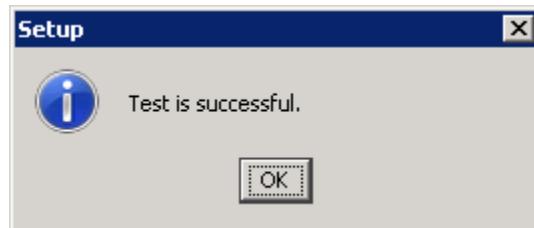
- c. Exit SQL Server Management Studio and return to the installation window.

29. Click Next after the Database has been created successfully.

The Runtime Database window opens.

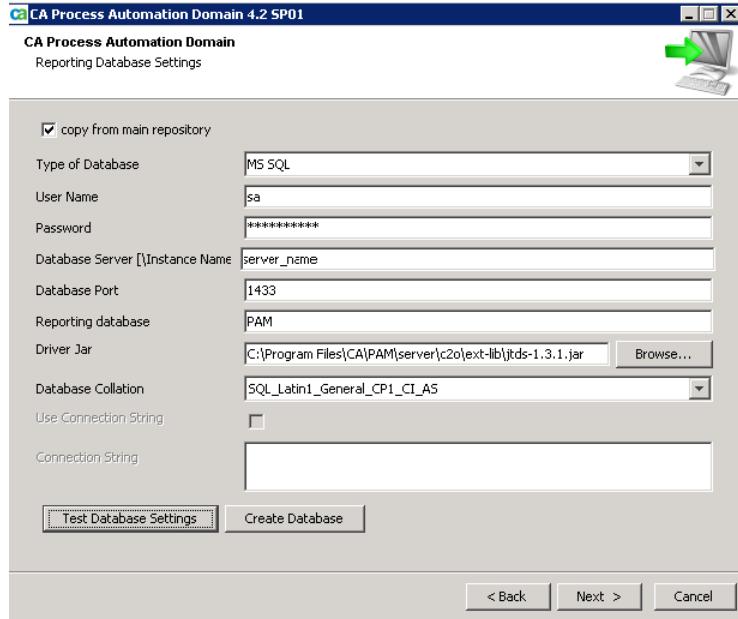


- a. Select the copy from main repository check box, on the Runtime Database window.
- b. Verify that the information is populated correctly from the Database Setting window.
- c. Click Test Database Settings and ensure that you receive a message indicating the test was successful.

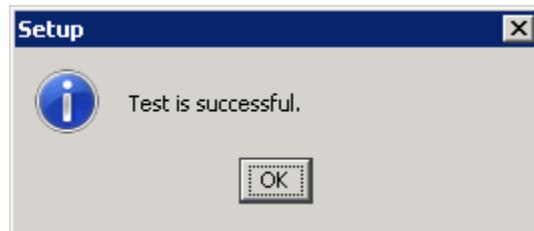


- d. Click OK to close the Setup window and return to the Runtime Database window.
30. Click Next.

The Reporting Database window opens.



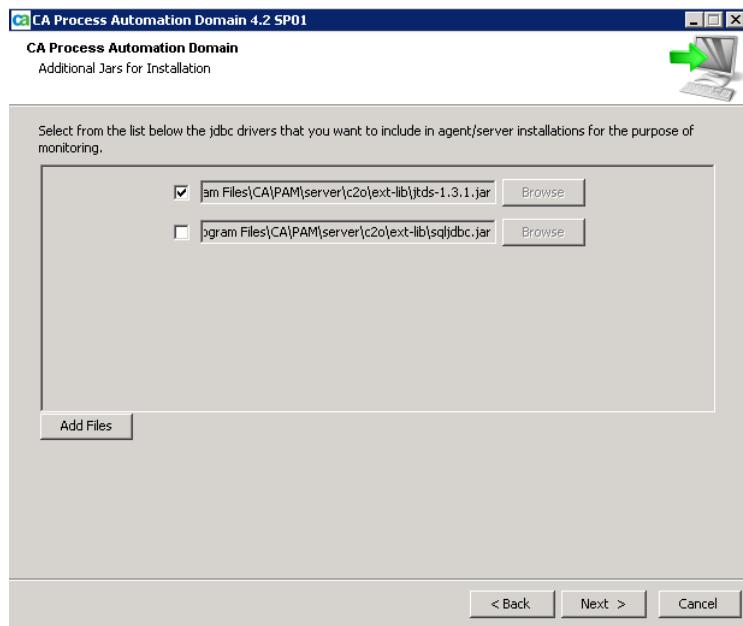
- a. Select the copy from main repository check box and verify that the information is populated correctly from the Database Setting window.
- b. Click the Test Database Settings button and ensure that you receive a message indicating the test was successful.



- c. Click OK to close the Setup window and return to the Reporting Database Settings window.

31. Click Next.

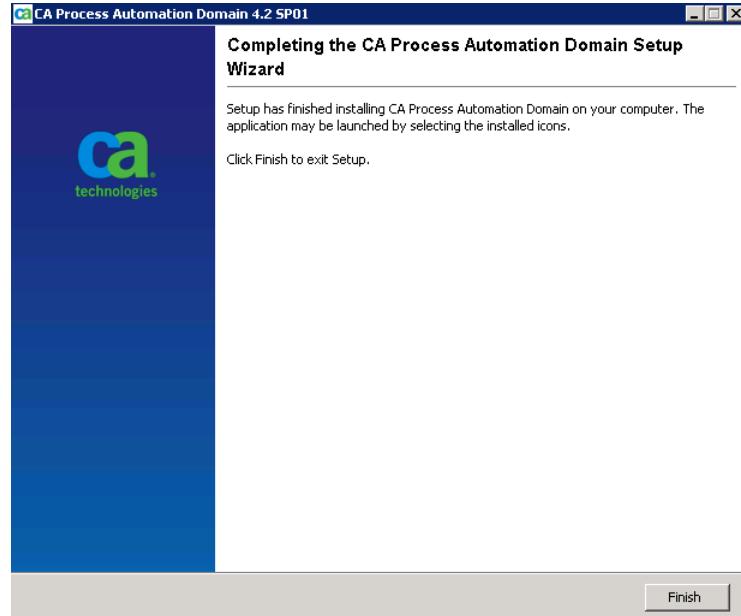
The Additional Jar for Installation window opens.



32. Select the check box and verify the location for the sqljdbc.jar file, then click Next.

The installation begins and takes several minutes to finish.

The Completing CA Process Automation Domain Setup wizard opens.

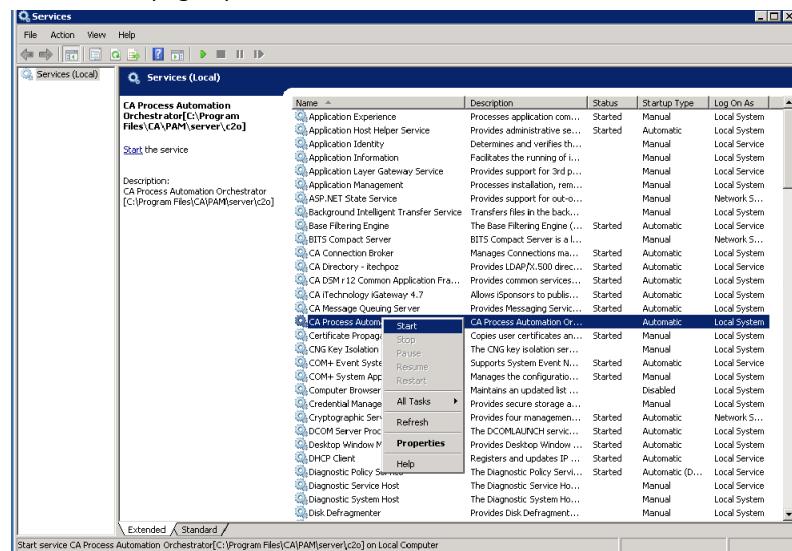


33. Click Finish.

The CA Process Automation component is installed.

34. Go to Start, Run, and Type services.msc.

The Services page opens.



35. Verify that Startup type for CA Process Automation service is set to Automatic.

- a. Right-click the CA Process Automation Orchestrator and select Start in the menu bar.

The service takes 5 to 10 minutes to start. The CA Process Automation service is set to start automatically whenever the server is started or rebooted.

The CA Process Automation installation is complete.

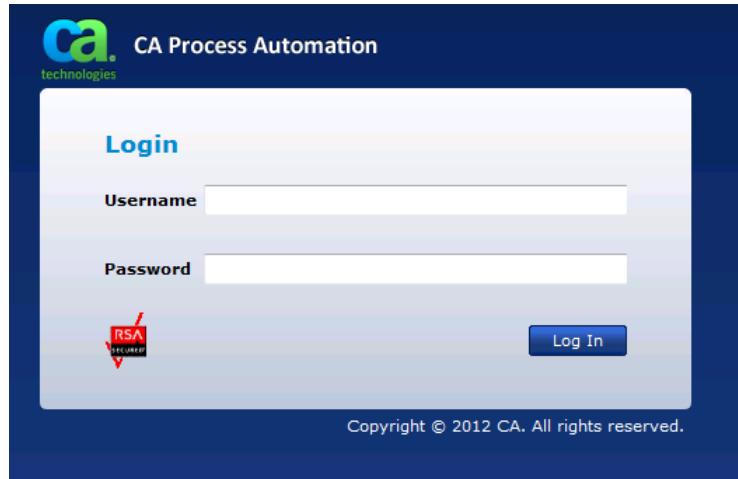
Verify Installation

Log in to verify the installation of CA Process Automation.

Follow these steps:

1. Do *one* of the following tasks:
 - Select Start, All Programs, CA, CA Process Automation Domain, Start CA Process Automation.
 - Type `http://<PAM_Server>:<Port_Number>`, in a browser and press Enter.

The Login page opens.



2. Log in to CA Process Automation as the Administrator (PAMAdmin).

If the login is successful, you verified the installation and access to CA Process Automation.

Verify CA EEM Application and Users

Log in to CA EEM and verify the users for CA Process Automation.

Follow these steps:

1. Open the CA EEM page.



2. Verify and select Process Automation from the Application drop-down.

This step verifies that the CA Process Automation application has been added to CA EEM.

3. Log in to CA EEM as the CA EEM Administrator (EiamAdmin).
4. Select Managed Identities, Users.

The Search Users page opens.

The screenshot shows the CA Embedded Entitlements Manager interface. The top navigation bar includes 'Home', 'Manage Identities' (which is selected), 'Manage Access Policies', and 'Configure'. Below the navigation is a breadcrumb trail: 'Users' > 'Groups'. The main content area has a 'Search Users' panel on the left with the following settings: Attribute: 'User Name', Operator: 'LIKE', and Value: (empty). A 'Go' button is at the bottom of this panel. To the right is a tree view of users, showing a top-level 'Users' node with two sub-nodes: 'Orphaned Users' and 'Users'. Under 'Users', there are four entries: 'pamdesigner', 'pamproducer', 'pamuser', and 'pamadmin'.

5. Select Application User Details.
6. Complete the following details, and click Go.

Attribute

Specifies the attribute for the search.

Value: User Name

Operator

Specifies the operator type.

Value: LIKE

Value

Specifies the value for the search. Leave this field blank.

If the PAMAdmin and PAMUser have been added to Active Directory or AD is not being used, then these users get listed under Users. If they are listed as Orphaned, then assign a CA Process Automation Administrator before continuing.

Add CA EEM User to the CA Process Automation Application

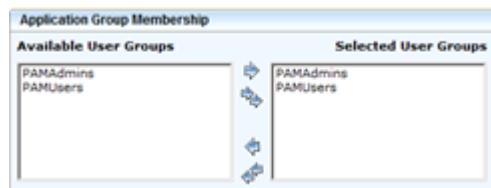
You can add CA EEM user to CA Process Automation to validate the credentials and information.

Follow these steps:

1. Select the user that you want to have access to the CA Process Automation application.
2. Click the Add Application User Details button.

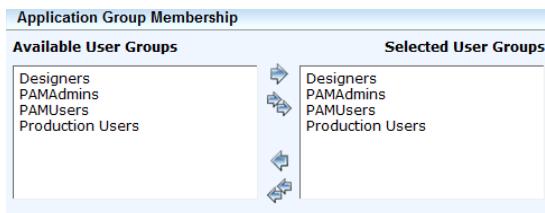
Example: pamadmin

The Application Group Membership window opens.



3. Perform the following steps under Application Group Membership:
 - a. Use the arrows to move the user from Available User Groups to Selected User Groups.

We recommend CA Process Automation Administrators be members of both User Groups.



- b. Use the arrows to move the user from Available User Groups to Selected User Groups.

We recommend CA Process Automation Users be members of CA Process Automation Users only.



4. Click Save.

After all of the CA Process Automation Administrators and Users have been set up, confirm the CA Process Automation Application Users.

5. Select Application User Details.
6. Complete the following details, and click Go.

Attribute

Specifies the attribute for the search.

Value: User Name

Operator

Specifies the operator type.

Value: LIKE

Value

Specifies the value for the search. Leave this field blank.



7. Verify that the Users with CA Process Automation access are listed.
8. Click Log Out to exit CA EEM.

You have added users to CA Process Automation.

Install CA ITCM

CA IT Client Manager with C1 patch is a grouping of three components—Asset Management, Remote Control, and Software Delivery. This section focuses only on installing Software Delivery. The Software Delivery component installs and removes software, including operating systems, on physical, and virtual computers.

First, you install the MDB which creates the database and loads it with various tables, then you Install CA IT Client Manager. This procedure completes the product installation and adds more tables to the database.

Best Practice: Always perform both installations even if SQL Server is located locally where Software Delivery is installed. Extra tables are created during each installation. If you are planning to install other CA products that use the MDB database, install the MDB first before installing the products.

See the installation procedure in the *CA IT Client Manager Implementation Guide*. You can download the *CA IT Client Manager Implementation Guide* from the CA Automation Suite for Clouds bookshelf.

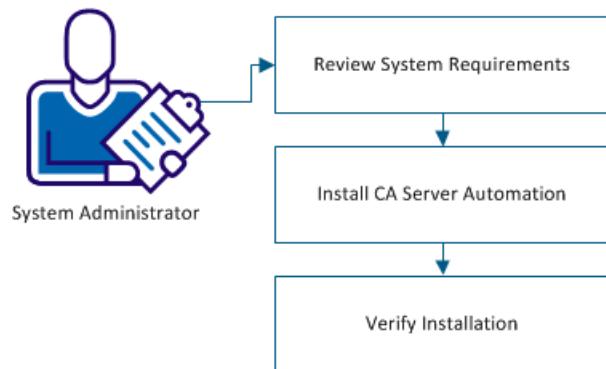
Install CA Server Automation

CA Server Automation is the component of CA Automation Suite for Clouds that monitors and manages data center resources, both physical and virtual. The component integrates and automates provisioning processes, standardizes configurations, and simplifies workflows to manage the complexity of continuously changing virtual environments.

Installing CA Server Automation also installs the CA Systems Performance for Infrastructure Managers (formerly known as CA SystemEDGE) agent that lets you remotely manage computers. The agent helps access information about the system configuration, status, performance, users, processes, and the file systems on the remote systems. The agent also enables reporting and managing exceptions, calculation of object severity, and status information. The CA Systems Performance for Infrastructure Managers agent must be installed on the remote system to fetch information about the system.

This following graphic illustrates the installation process:

How to Install CA Server Automation



This section contains the following topics:

1. [Review Prerequisites](#) (see page 112).
2. [Install CA Server Automation](#) (see page 113).
3. [Verify Installation](#) (see page 132).

Review Prerequisites

Refer to the Review System and Hardware Requirements section for general installation requirements. Complete and verify the following requirements before you begin the installation:

CA Server Automation must be installed on a dedicated server.

The following applications must be installed on the server where CA Server Automation is installed:

- Microsoft SQL Server 2008 R2 x 64 Standalone in Mixed Authentication Mode.
- Java JDK Version 1.7 or above (64 bit)
- CA EEM without FIPS mode enabled.
- Adobe Acrobat Reader 9.0 and above.

You must have a working knowledge of the following tools before you can install CA Server Automation:

- Apache Tomcat.
- Microsoft SQL Server.

Check Administrator Privileges

You must be in the local administrator group to install CA Server Automation. Capture the login and other necessary details on the [installation worksheet](#) (see page 19).

Before you install CA Server Automation, you must have the administrator login credentials for the following applications:

- CA EEM

CA Server Automation uses CA EEM to manage the common access policy, user authentication, and authorize service offerings to users.

- Microsoft SQL Server

CA Server Automation uses the Microsoft SQL Server database to store and retrieve user and management data.

Install CA Server Automation

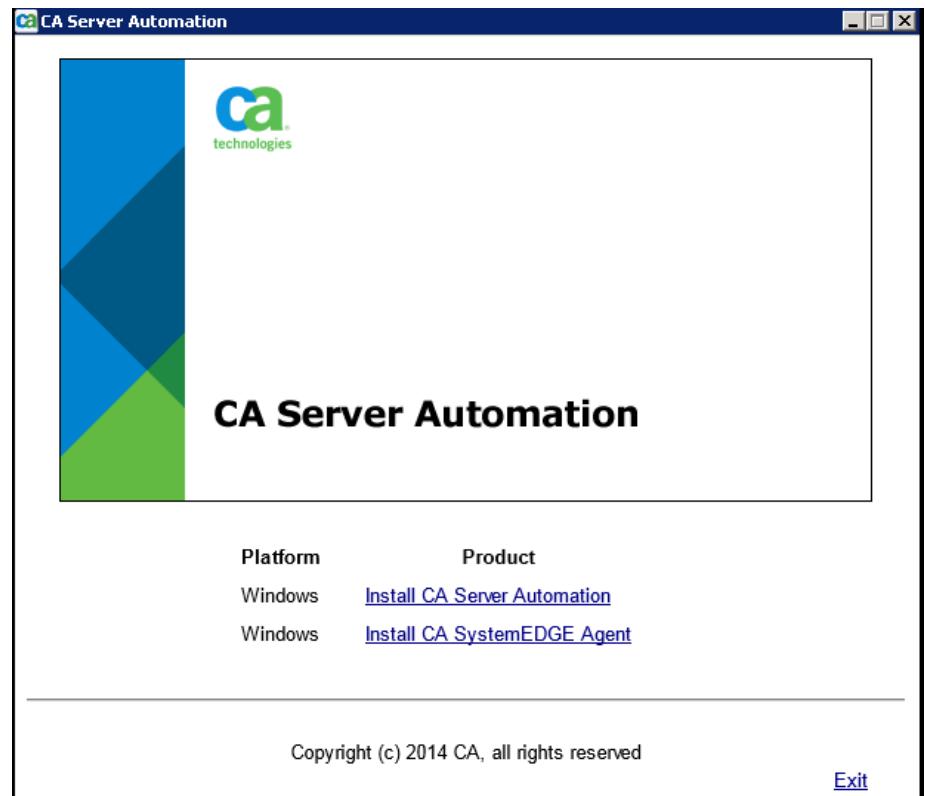
This procedure describes how to install the CA Server Automation component of CA Automation Suite for Clouds.

Follow these steps:

1. Download the CA Server Automation 12.8.2 media from CA Support Online.
2. Extract the CA Server Automation ISO file to the CA Server Automation folder.

3. Double-click setup.hta to start the installation.

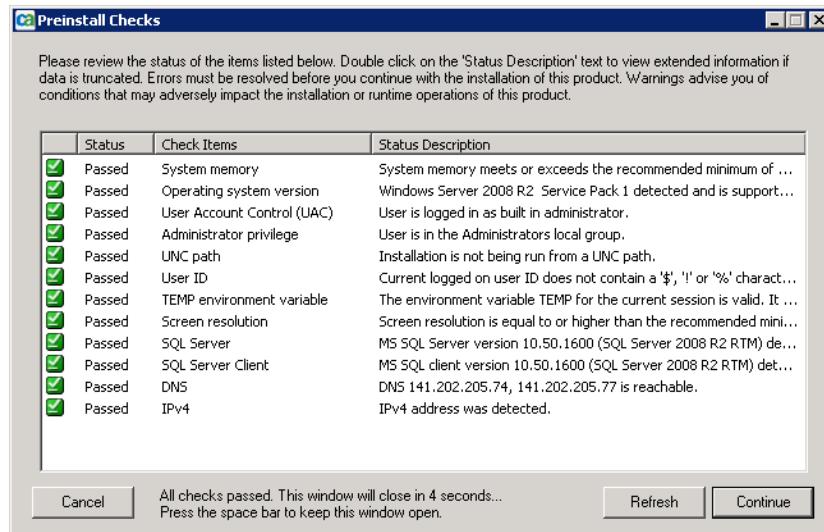
The CA Server Automation window opens.



Note: The CA SystemEDGE Agent is installed with the CA Server Automation installation. If you choose to install the CA SystemEDGE Agent later, clear the installation option for the agent during this installation process.

4. Click Install CA Server Automation.

The Preinstall Checks window opens.



If you see the status of any item as Failed, review the Status Description and take an appropriate action.

5. Review the Preinstall items and click Continue.

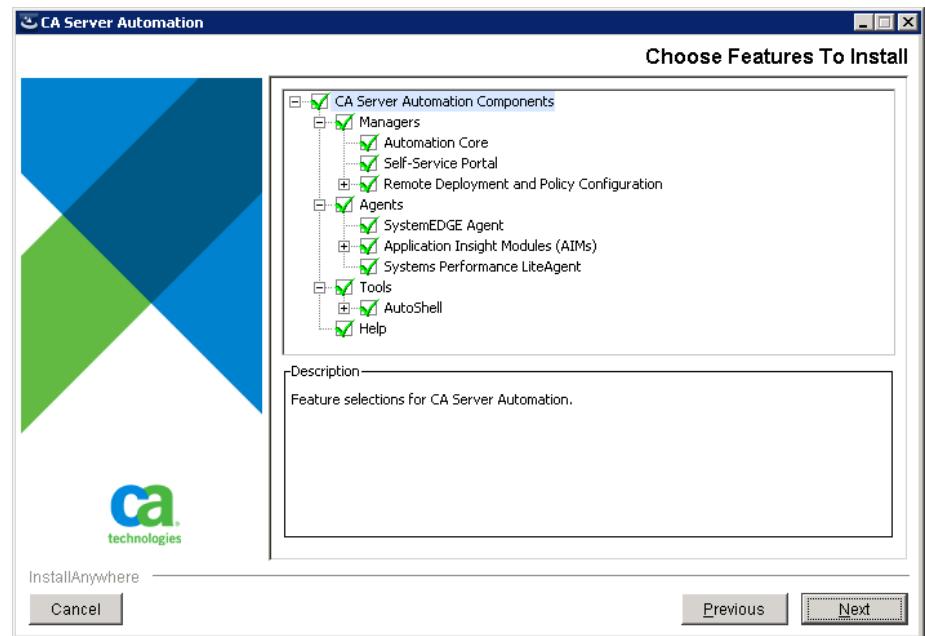
The Introduction window opens.

6. Click Next.

The License Agreement window opens.

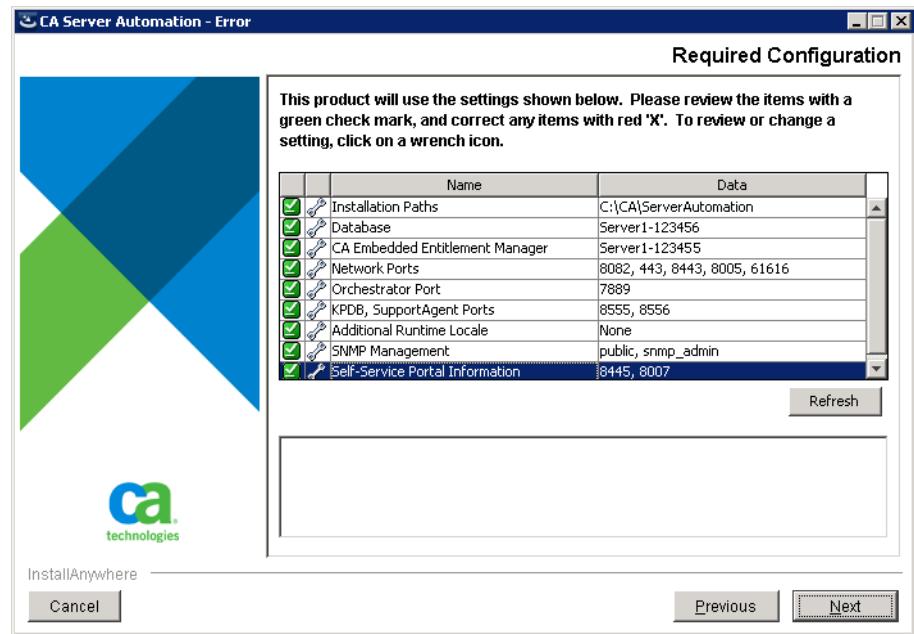
7. Scroll to the bottom of the License Agreement window. Select I accept the terms of the License Agreement, and click Next.

The Choose Features To Install window opens.

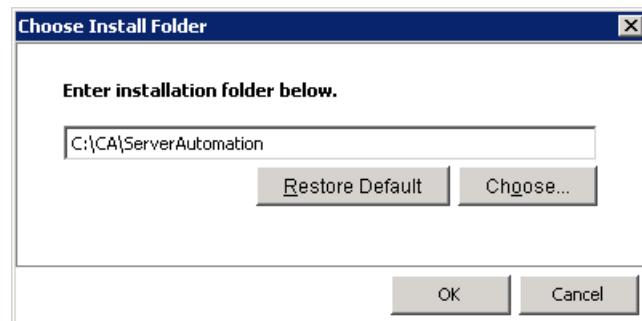


8. Accept the defaults and click Next.

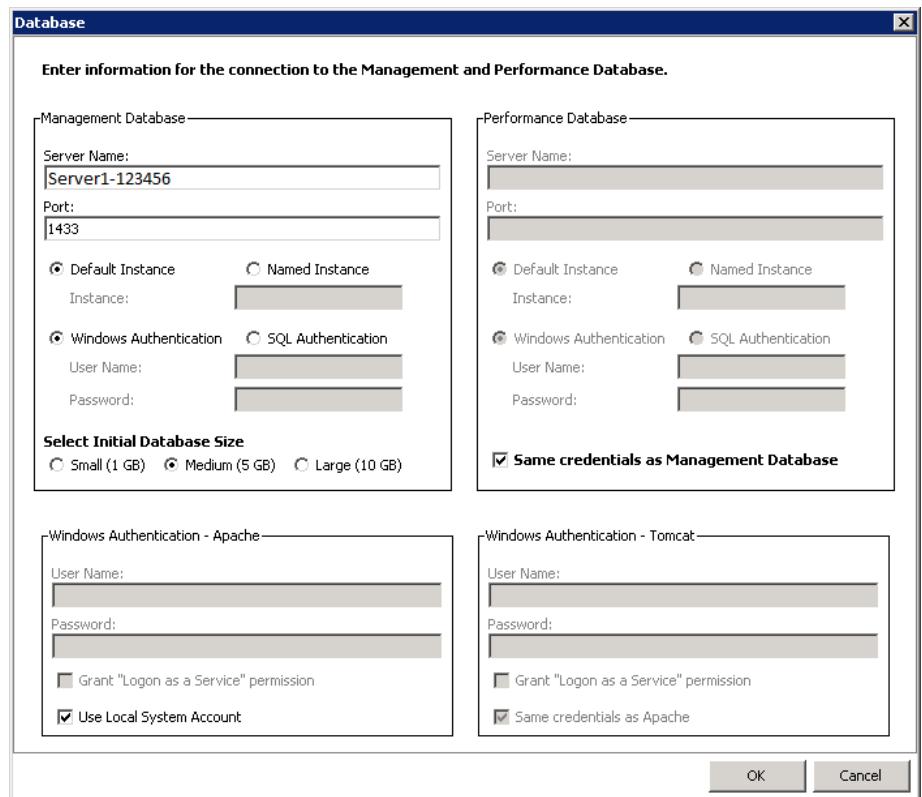
The Required Configuration window opens.



9. (Optional) Double-click Installation Path to change the installation location and click OK to return to the Required Configuration window.



10. Double-click Database to change database connection settings, Apache, and Tomcat authentication details.



Management Database

The Management DB is a common data repository for all managed objects, which are based on a model for describing management data. The Management DB stores information about servers, services, rules, actions, virtual platform objects, events, alerts, and relationships among these objects.

Server Name

Specifies the host name of the server where the database is installed.

Port Number

Specifies the port number of the server.

Default: 1433

Default Instance

Specifies that you want to use the default instance of the database.

Named Instance

Specifies that you want to use the named instance of the database. Type the instance name that you have provided while installing the database.

Instance

Specifies the instance name, when a named instance of the database is used.

Windows Authentication

Specifies that you want to use the Windows authentication credentials to log in to the database. Select Windows Authentication, if you have selected it while installing the database.

SQL Authentication

Specifies that you want to use the SQL authentication credentials, when the named SQL database is installed.

Select Initial Database Size

Specifies the initial database size depending on the expected usage.

Performance Database

The Performance DB is a repository that stores all the metrics that are collected from the servers in your data center.

The data that is stored in this database is used for various functions. For example, this DB is the source of the data that is used to create historical reports. CA Server Automation also uses the data in this database and user-created rules to make logical business decisions.

Select Same Credentials as Management Database to use management database login credentials for the performance database.

Windows Authentication - Apache

Apache is a web server on which CA Server Automation runs.

- Specify the Apache log in credentials.
- Select Use Local System Account if the local system account is used to log in to Apache.

Windows Authentication - Tomcat

Tomcat is an application server that provides software applications with the following services:

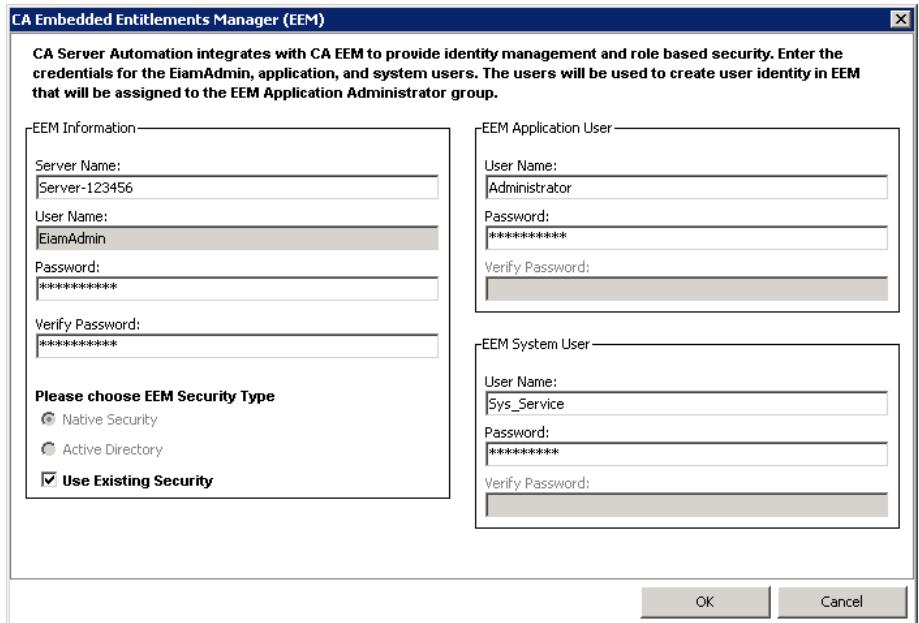
- Security
- Data services
- Transaction support
- Load balancing
- Management of large distributed systems

CA Server Automation uses Tomcat for running its services.

Specify the Tomcat log in credentials.

Select Same credentials as Apache if the Apache account is used to log in to Tomcat.

11. Click OK to return to the Required Configuration window.
12. Double-click CA Embedded Entitlements Manager to configure CA EEM authentication details. Modify the populated fields as needed, then click OK to return to the Required Configuration window.



EEM Information

Specifies the CA EEM server administrator authentication information.

Server Name

Specifies the server on which CA EEM is installed.

User Name

Specifies the user name to log in to the server where CA EEM is installed.

Default: EiamAdmin

Password

Specifies the password.

Verify Password

Specifies the password for verification.

Note: Password and Verify Password must match the passwords used when you installed CA EEM.

EEM Application User

Specifies the CA EEM application user authentication information.

User Name

Specifies the user name.

Default: Administrator

Note: Ensure user exists in CA EEM.

Password

Specifies the password.

Verify Password

Specifies the password for verification.

EEM System User

Specifies the CA EEM system user authentication information. These credentials are used to log in to CA Server Automation.

User Name

Specifies the user name.

Default: sys_service

Note: Ensure user exists in CA EEM.

Password

Specifies the password.

Verify Password

Specifies the password for verification.

Please choose EEM Security Type

Native Security

Specifies that the user authentication is done locally using CA EEM.

Active Directory

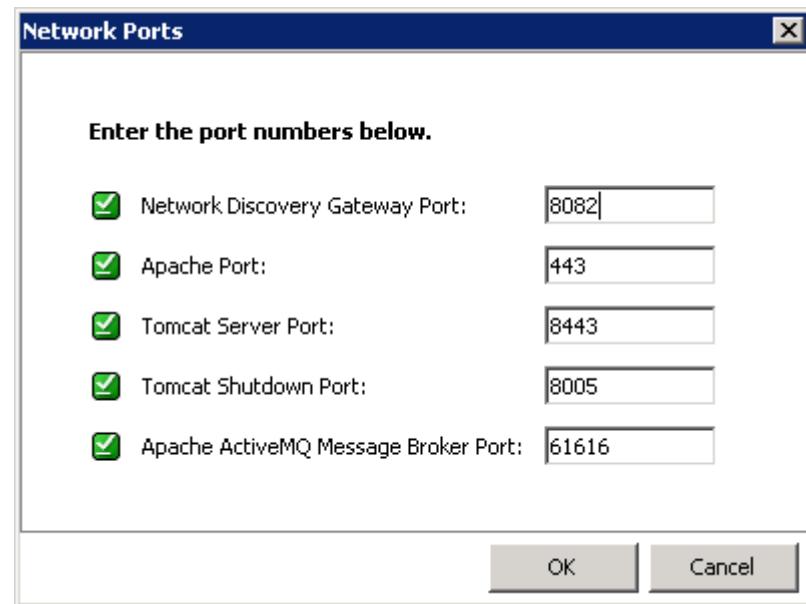
Specifies the Active Directory option for user authentication. Select this option if CA EEM is integrated with Microsoft Active Directory.

Use Existing Security

Indicates to use the existing security for authentication. Select the Use Existing Security check box.

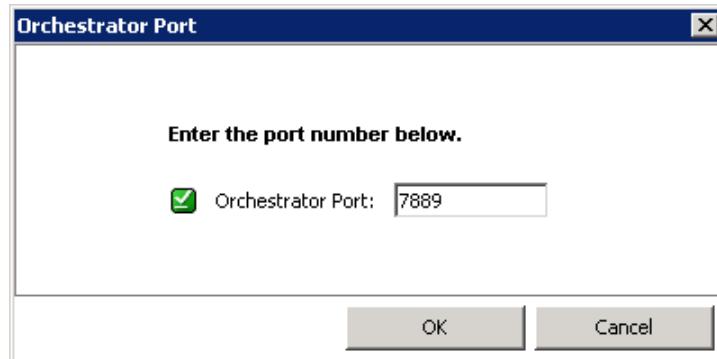
13. Double-click Network Ports to verify the network port numbers.

The port numbers must match port numbers that are given on the Network Ports screen. If a port is in use by another service, the dialog displays it in Red. Change the port information accordingly.



14. Click OK to return to the Required Configuration window.
15. (Optional) Double-click Orchestrator port to verify port numbers.

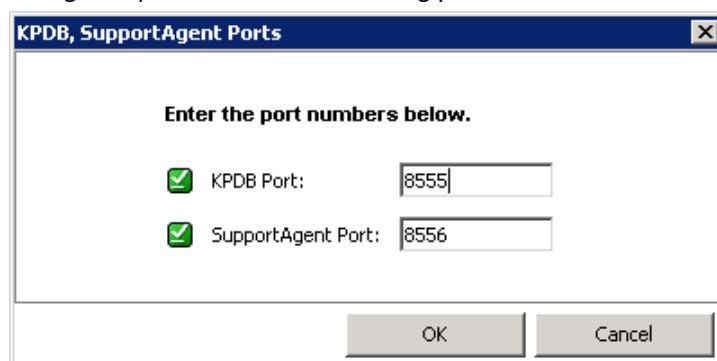
The port numbers must match port numbers that are given on the Orchestrator Port screen. If a port is in use by another service, the dialog displays it in Red. Change the port information accordingly.



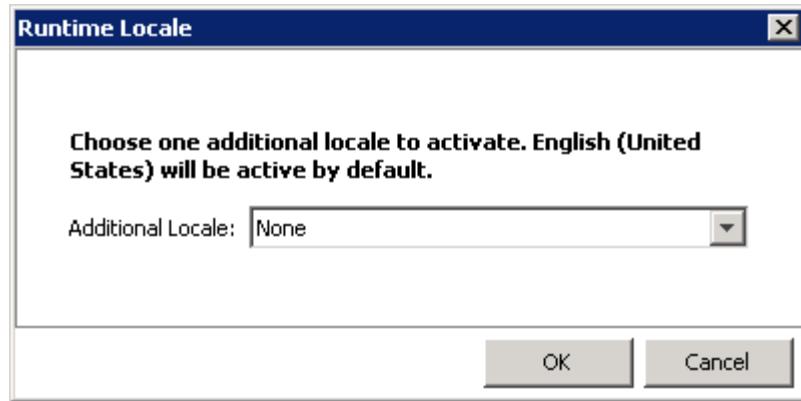
16. Click OK to return to the Required Configuration window.
17. (Optional) Double-click KPDB, SupportAgent Ports to verify the port numbers.

The port numbers must match port numbers that are given on the screen.

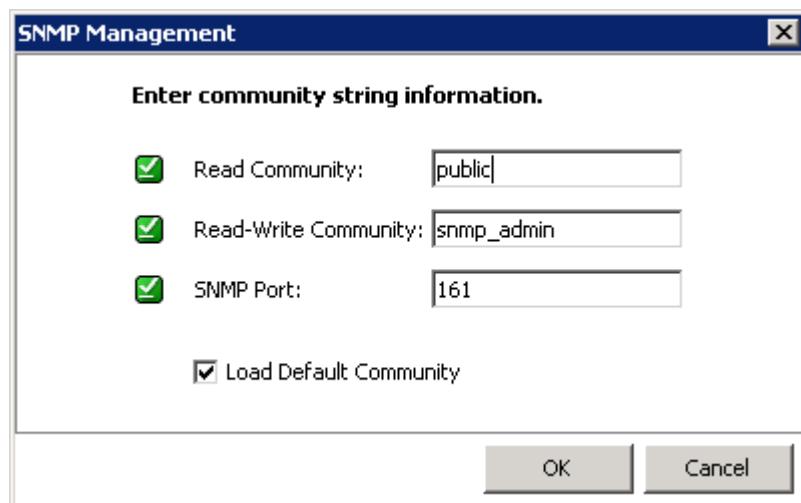
If a port is in use by another service, the dialog displays it in Red. Change the port information accordingly.



18. Click OK to return to the Required Configuration window.
19. (Optional) Double-click Additional Runtime Locale to activate another language.

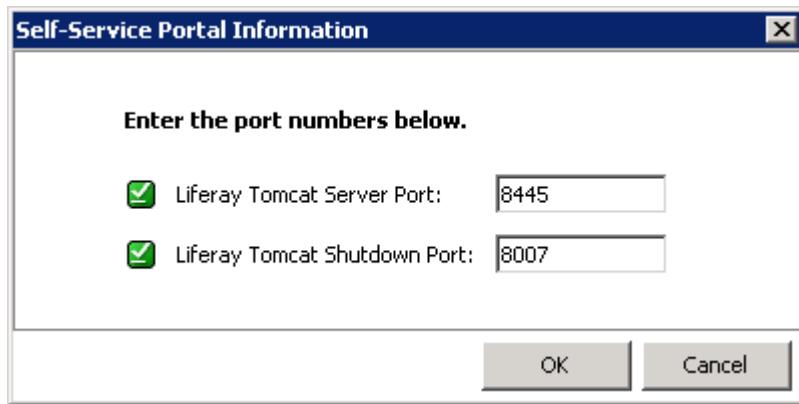


20. Select an additional language and click OK to return to the Required Configuration window.
21. (Optional) Double-click SNMP Management to verify the community string information.



CA Server Automation uses Simple Network Management Protocol (SNMP) for monitoring the network. If a port is in use by another service, the dialog displays it in Red. Change the port information accordingly.

22. Click OK to return to the Required Configuration window.
23. (Optional) Double-click Self-Service Portal Information to verify Tomcat port numbers.

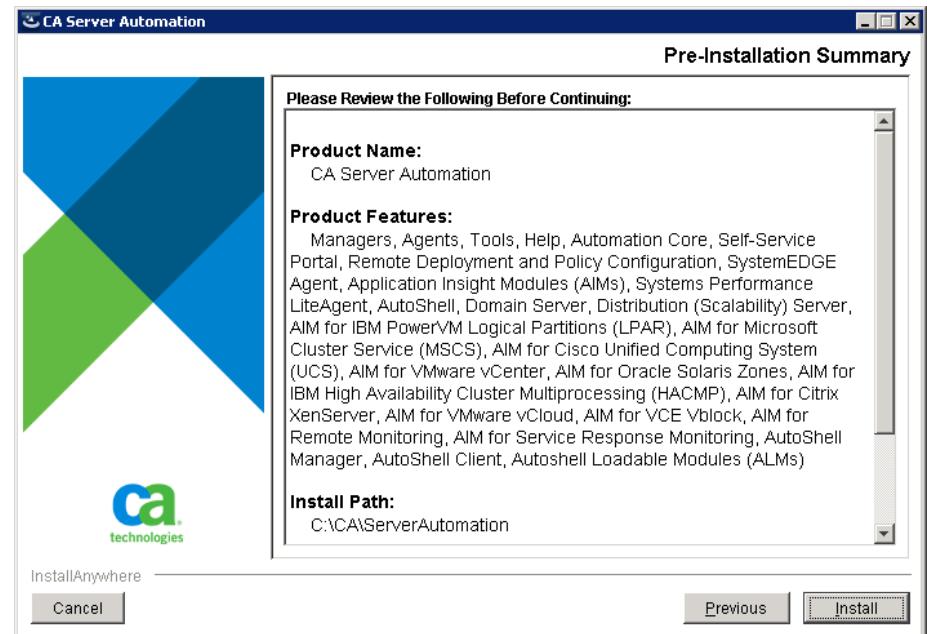


Note: Liferay is a self-service portal on which Tomcat runs. If a port is in use by another service, the dialog displays it in Red. Change the port information accordingly.

24. Click OK to return to the Required Configuration window.

25. Click Next.

The Pre-Installation Summary window opens.

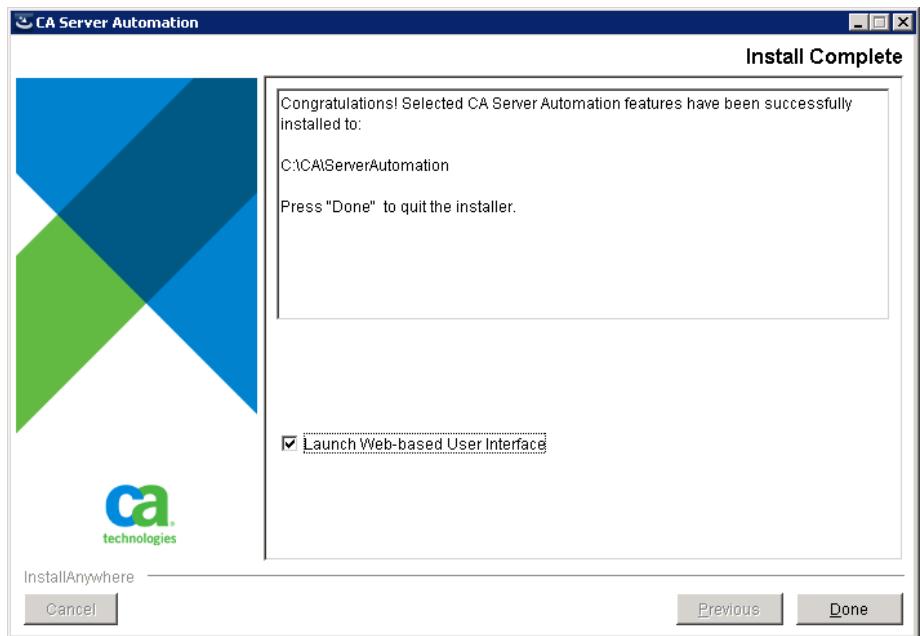


26. Scroll down to the bottom of the Pre-Installation Summary window to review the installation summary and click Install, if information is correct.

The Installing CA Server Automation window opens and when the installation is complete the Installation Complete window opens.



Note: The installation takes several minutes to complete.



27. Select Launch Web-based User Interface and click Done.

CA Server Automation is installed on the local host and the Login page opens.

Verify Installation

You can launch CA Server Automation to verify that it is installed successfully.

Follow these steps:

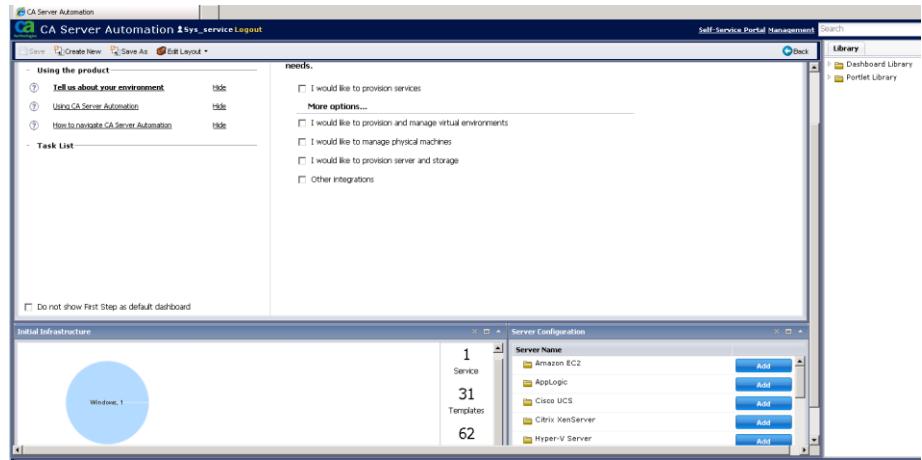
1. Click Start, All Programs, CA, CA Server Automation, Launch CA Server Automation.

The CA Server Automation Login window opens.



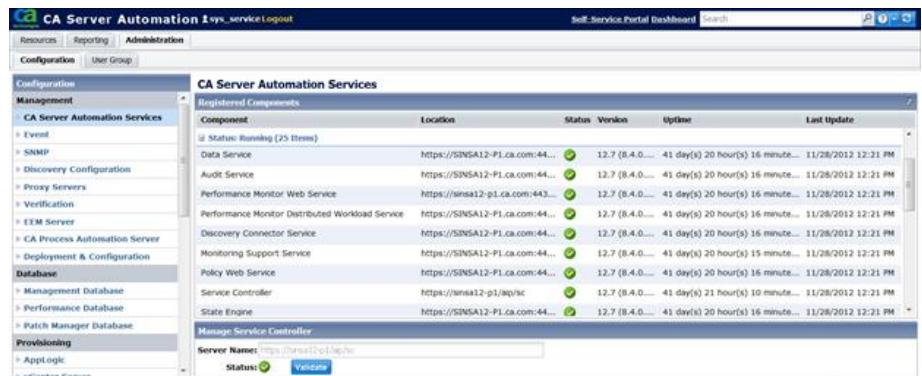
2. Log in to CA Server Automation with the default username (sys_service) and the password you set for the CA EEM System User when you installed CA Server Automation.

The CA Server Automation dashboard opens.



3. Click Management, Administration.

The CA Server Automation Services page displays a list of services. If all the services are running, the installation was successful.



4. Click Logout to close the CA Server Automation.

You have verified that CA Server Automation is installed.

You have installed CA Server Automation and verified the installation by checking the list of available services.

Install CA Service Catalog

CA Service Catalog is a component of CA Automation Suite for Clouds. The component is an enterprise cloud automation solution that is designed to assist you in delivering cloud services.

The component is a single point of contact to a virtualized service environment. The component defines and measures your services, provides service approval and provisioning while automating and tracking service delivery across resources. This component provides financial and strategic insight into service consumption.

The CA Service Catalog consists the following components:

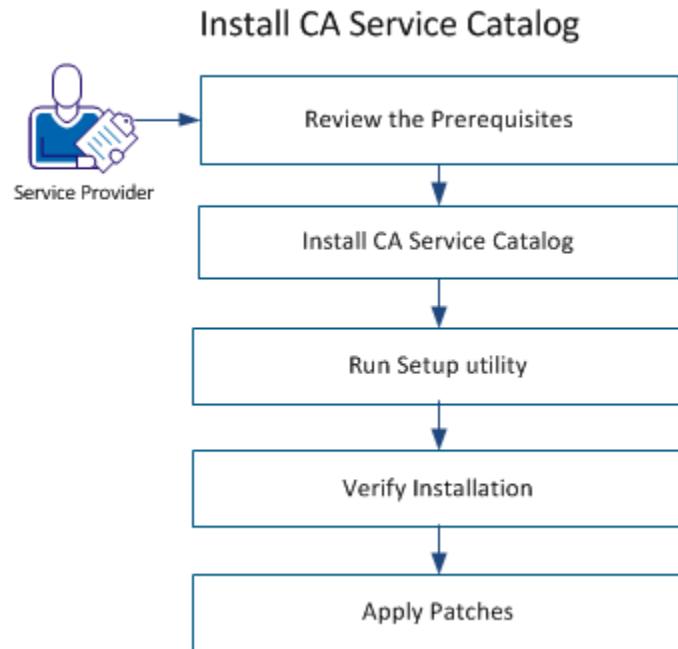
CA Service Catalog

Displays the services and forms to the user.

CA Service Accounting

Tracks services, gathers reports, and displays the account details. This component is used for billing purposes.

The following diagram illustrates how a Service Provider installs the product and its components:



To complete the installation, follow these steps:

1. [Review the Prerequisites](#) (see page 135).
2. [Install CA Service Catalog](#) (see page 136).
3. [Run Setup Utility](#) (see page 141).
4. [Verify Installation](#) (see page 151).
5. [Apply Patches](#) (see page 152).

Review the Prerequisites

Refer to the Review System and Hardware Requirements section for general installation requirements. Complete and verify the following requirements before you begin the installation:

- Microsoft SQL Server 2008 R2 is installed.

Note: CA Automation Suite for Clouds does not support Oracle.

- Microsoft SQL Client is installed.
- CA EEM is installed.

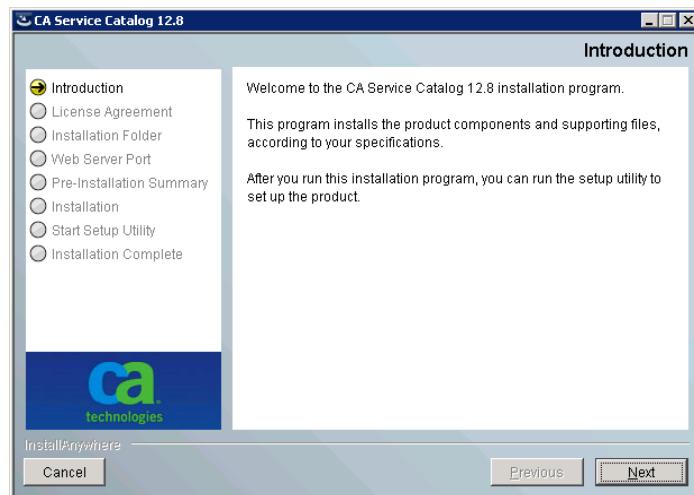
Install CA Service Catalog

CA Service Catalog acts as a dashboard for the activities you perform on Service View and CA Service Accounting.

Follow these steps:

1. Open the CA Service Catalog r12.8 media file.
2. Right-click CA_Service_Catalog.exe and select Run as an administrator.

The installation wizard opens.

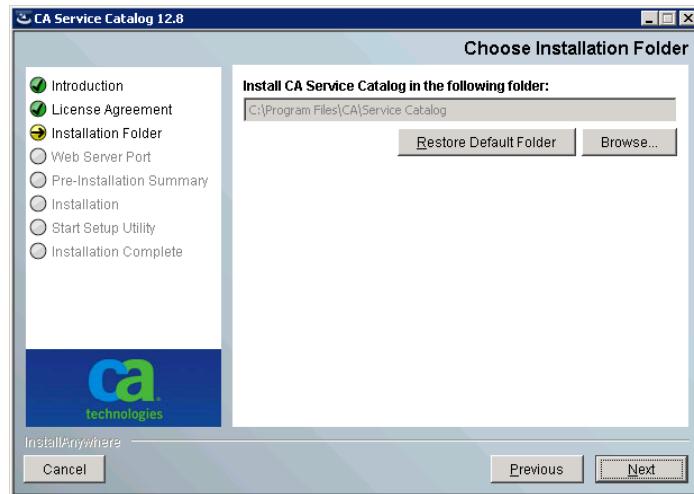


3. Select Next.

The License Agreement page opens.

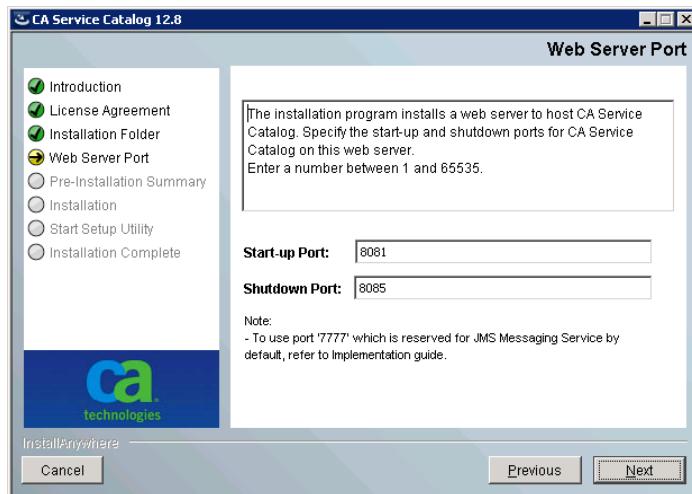
4. Read the license agreement, select I accept the terms in the license agreement, and click Next to continue.

The Choose Installation Folder page opens.



5. Click Browse to change the installation folder or Accept the default installation folder and click Next.

The Web Server Port page opens.



6. Type the Start-up and Shutdown port numbers for CA Service Catalog services.

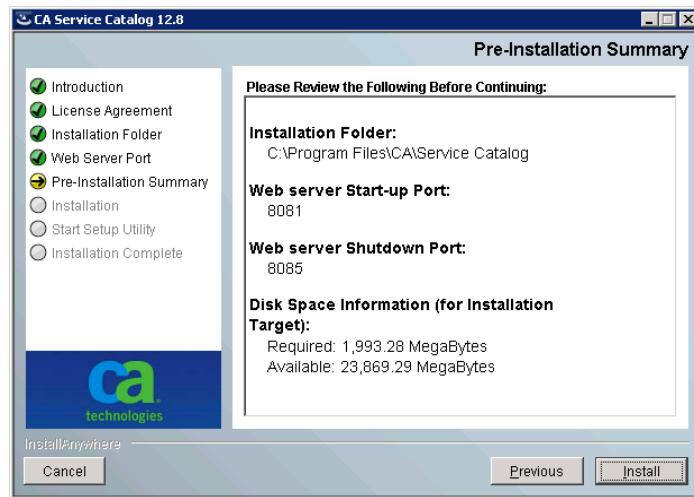
Important! Ensure the port is not in use by any other service. We recommend that you do not use port 7777 as the startup or shutdown port. Port 7777 is reserved for Java Messaging Service (JMS).

If you must use port 7777, reset the JMS port number after you have finished running the setup utility. Otherwise, port conflicts occur, and the product does not function correctly.

Note: No host name is needed because you install the product locally.

7. Click Next.

The Pre-Installation Summary page opens.

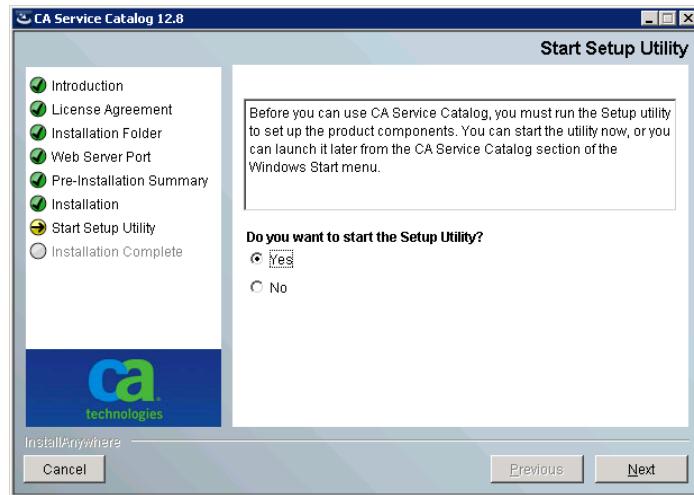


8. Click Install.

[Install CA Service Catalog](#)

The CA Service Catalog installation begins and usually takes several minutes to complete.

The Start Setup Utility page opens.



9. Select Yes, and click Next.

Wait for the installer to configure CA Service Catalog. The installation may take few minutes to complete.

The Installation Complete page opens.



10. Click Done.

The installer executes the CA Service Catalog Run Setup Utility.

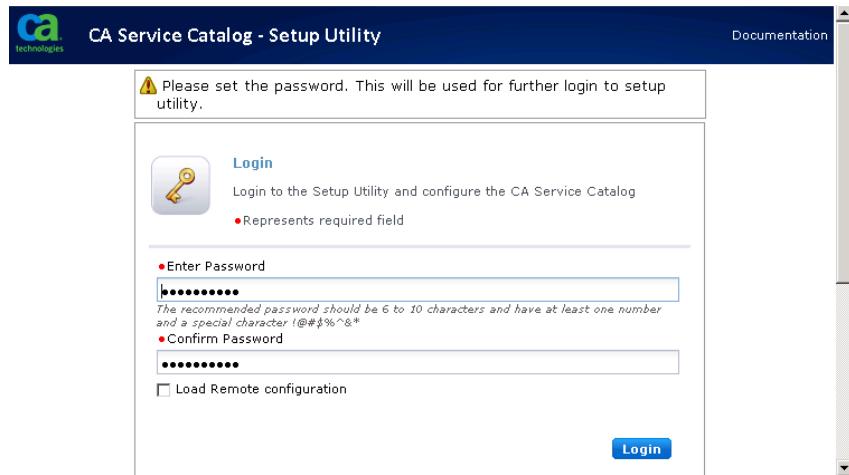
Run Setup Utility

Run the CA Service Catalog setup utility to set up your database, configure CA EEM, and install the product components. The components are Catalog Component, Catalog Content, and Accounting Component.

Follow these steps:

1. Click Start, All Programs, CA, Service Catalog, Service Catalog - Launch Setup Utility.

The Setup Utility page opens.



2. Type the password and confirm the password.

Important! Record the password in the [Installation Worksheet](#) (see page 19) for reference, because the utility requires you to specify the password each time you start it.

3. (Optional) Select Load Remote Configuration, if CA Service Catalog is set up on another server and you want to use the same setup on this server.
4. Click Login.

You have successfully logged in to CA Service Catalog Setup Utility.

The Deploy catalog database and configure page opens.

Set up Database Module

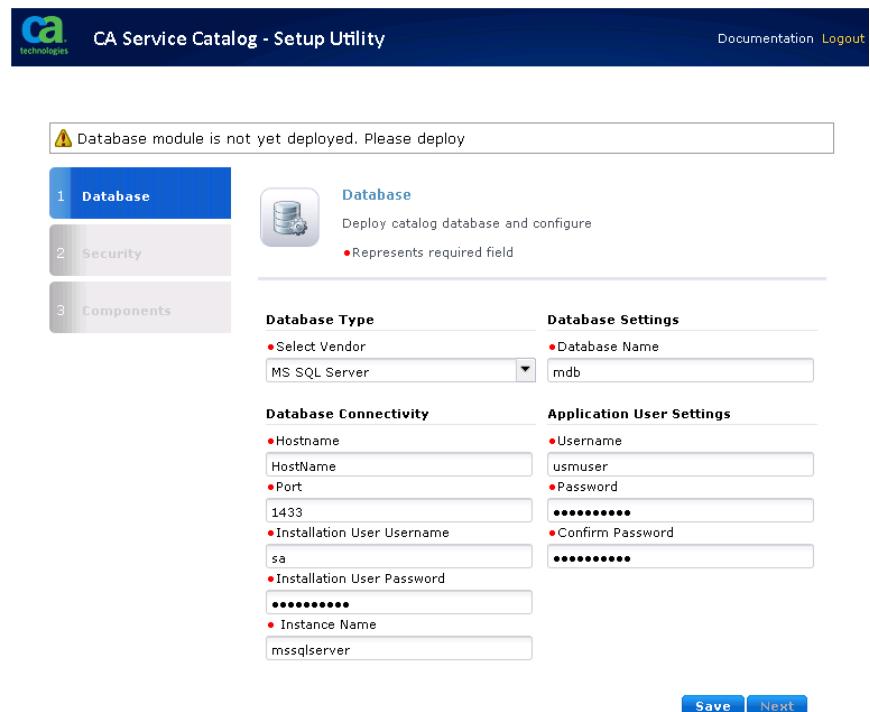
Set up the database so that the CA Service Catalog users and the catalog system can function correctly.

Follow these steps:

1. Select the database to connect from the Database Type drop-down list.

Select Vendor

Specifies the database software vendor.



The screenshot shows the CA Service Catalog - Setup Utility interface. The title bar includes the CA technologies logo, the title 'CA Service Catalog - Setup Utility', and links for 'Documentation' and 'Logout'. The main content area has a header 'Database' with a warning message: '⚠ Database module is not yet deployed. Please deploy'. Below this, a navigation bar shows '1 Database' (selected), '2 Security', and '3 Components'. The 'Database' section contains a 'Database' icon and the text 'Deploy catalog database and configure'. A note '● Represents required field' is present. The 'Database Type' section shows 'Select Vendor' set to 'MS SQL Server'. The 'Database Settings' section shows 'Database Name' set to 'mdb'. The 'Database Connectivity' section shows 'Hostname' set to '1433', 'Port' set to '1433', 'Installation User Username' set to 'sa', and 'Installation User Password' (redacted). The 'Application User Settings' section shows 'Username' set to 'usmuser', 'Password' (redacted), 'Confirm Password' (redacted), and 'Instance Name' set to 'mssqlserver'. At the bottom are 'Save' and 'Next' buttons.

2. Verify or complete the fields in the Database Connectivity section:

Hostname

Specifies the computer name of the Microsoft SQL Server (SQL Server).

Default: localhost

Port

Specifies the TCP Port number of the database server.

Default: 1433

Installation User Username and User Password

Specifies the user name and password of the SQL Server database administrator (DBA). The setup utility uses these credentials to set up the CA Service Catalog database.

Default Username: sa

Instance Name

Defines the SQL Server instance name for the MDB. For example, myinstance. You can specify either a primary instance or a named instance.

3. Specify the name of the CA Service Catalog database, In the Database Settings section, typically MDB.

Database Name

Specifies the name of the CA Service Catalog database.

Default Database Name: mdb

To install the CA Service Catalog database schema into an existing database, specify the name of that database.

Follow these guidelines:

- If you plan to integrate CA Service Catalog with any other CA product that uses the MDB, specify mdb as the database name.
- If you want CA Service Catalog to run on its own database, you can specify a different database name other than mdb. To integrate with other CA products in the future, use the setup utility to change your custom database name to mdb.
- For an upgrade, use the same database name as you used for the previous release. Most likely, this name is mdb.

4. Specify the Application User Settings.

Username and Password fields

Specifies the user name and password for accessing this database.

The user name and password are created in the database. CA Service Catalog uses this user name and password to connect to the database.

Important! Record the passwords for reference in the [Installation Worksheet](#) (see page 19).

5. Click Save.
6. Click OK when prompted to confirm the deployment of the database on host.
7. Click OK when prompted to restart the database service for changes to take effect.

A confirmation message appears. The database setup takes several minutes to complete.

The CA Service Catalog database setup is complete.

Configure Security Module

After the database is set up, configure CA EEM for use with CA Service Catalog in the security module.

Follow these steps:

1. Click the Security tab on the left menu.

The Security page opens.

CA Service Catalog - Setup Utility

Documentation Logout

1 Database

2 Security

3 Components

Security

Configure EEM for CA Service Catalog authentication and authorization

● Represents required field

● Host Name
Hostname

● Application Instance Name
CA Service Catalog

● Admin Username
EiamAdmin

● Admin password

Save Next

2. Confirm or update the following information:

Host Name

Specifies the host name of the server on which CA EEM is installed.

Default: localhost

Application Instance Name

Specifies the CA Service Catalog instance name for CA EEM.

Default: CA Service Catalog

Admin Username

Specifies the CA EEM administrator user name.

Default: EiamAdmin

Admin Password

Specifies the CA EEM administrator password.

Important! Record the password for reference in the [Installation Worksheet](#) (see page 19).

3. Click Save.
4. Click OK when prompted to confirm the deployment of the CA EEM application instance on host.
5. Click OK, when prompted to restart the service for changes to take effect.

A confirmation message appears. The utility creates the required CA Service Catalog objects in CA EEM. Examples include the Service Catalog application, policies, and users (including spadmin).

You have configured CA EEM for use with CA Service Catalog.

Note: In case you are upgrading CA Service Catalog, continue with steps in [Upgrade CA Service Catalog](#) (see page 292) section.

Configure the Product Components

After configuring CA EEM with CA Service Catalog configure the product components that you want on this computer.

1. Click the Components tab on the left menu.

The Components page opens.

None of the components are deployed yet.

Components

Configure Catalog and Accounting components

● Represents required field

Business Unit

CA technologies

Name of the root business unit. Once configured can not be altered.

Catalog

Content

<input checked="" type="checkbox"/> Select/Deselect All	<input checked="" type="checkbox"/> Network Services
<input checked="" type="checkbox"/> Application Services	<input checked="" type="checkbox"/> Personnel Services
<input checked="" type="checkbox"/> Corporate Services	<input checked="" type="checkbox"/> Project Services
<input checked="" type="checkbox"/> Facilities Services	<input checked="" type="checkbox"/> Reservation Services
<input checked="" type="checkbox"/> IT Services	<input checked="" type="checkbox"/> Telecom Services

Accounting

Save **Finish**

2. Type the name of the business unit.

Note: You cannot modify the business unit name after it is assigned using the setup utility. The business unit name is not editable when CA Service Catalog is upgraded from an earlier version. The existing business unit name appears as a read-only field. You can change the business unit name using the CA Service Catalog UI.

3. Select the components that you want to use on this computer:

Catalog Component

Enables you to create service options and service option groups, which you can use to create services that users can request from the catalog.

This option includes the Catalog Content, which supplies the predefined services in the catalog. Examples include services for requesting hardware, software, and other IT essentials from your business unit. You can use these services as-is, or you can copy and customize them.

This option installs a Windows service named CA Service Catalog.

Accounting Component

Provides the billing and chargeback for the services that users request from the catalog. You can also use Accounting Component to allocate costs, prepare budgets, and plan the IT services.

This option installs a Windows service named CA Service Accounting.

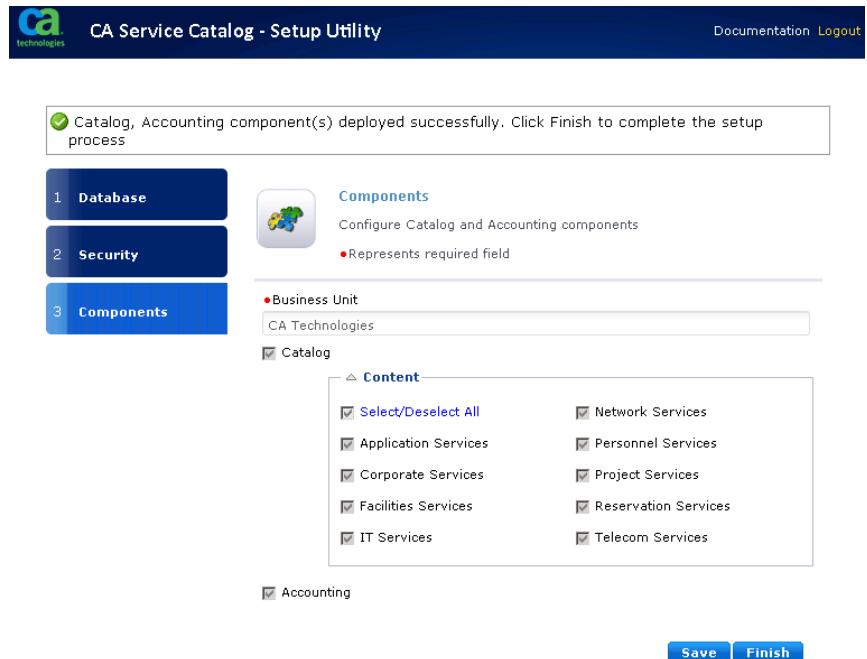
4. Click Save.

5. Click OK, when prompted to confirm the selection.

The catalog deployment can take several minutes to complete.

Install CA Service Catalog

A confirmation message appears on the successful deployment.



6. Click Finish.
7. Click OK when prompted to restart the service.
A confirmation message appears when services are restarted successfully.
8. Click Launch CA Service Catalog, when prompted, to open the CA Service Catalog login page.
You have successfully deployed CA Service Catalog and its components.

Verify Installation

Log in to CA Service Catalog and verify that the component is installed.

Follow these steps:

1. Do *one* of the following tasks:

- Select Start, All Programs, CA, Service Catalog, Service Catalog - Web Client.
- Type `http://<Catalog_Server>:<Port_Number>` in a browser and press Enter.

The Login page opens.

2. Log in to CA Service Catalog as an administrator.

Default User Name: spadmin

Default Password: spadmin

The CA Service Catalog Dashboard opens.

3. Verify that the Home page has the following tabs:

- Home
- Catalog
- Accounting
- Administration

If you can log in and access the CA Service Catalog services, the installation was successful.

Apply Patches

To enable CA Service Catalog to work with CA Automation Suite for Clouds, apply patches to your installation.

Follow these steps:

1. Log in to <https://ca.com/support> with your credentials.
2. Click Download Center, search for and download the following patches:
 - CP03
 - RO70135
3. Extract the zip files and run the .exe file.

The patch is applied.

You have successfully completed installing CA Service Catalog and the required patches.

Chapter 4: Configure the Components

Use the configuration procedures in the same order as described in this chapter for configuring and importing several content packs for the CA Automation Suite for Clouds Base Configuration.

This section contains the following topics:

- [Integrate CA Service Catalog with CA Server Automation](#) (see page 154)
- [Integrate CA Service Catalog with CA Process Automation](#) (see page 155)
- [Configure CA Process Automation with Active Directory Server](#) (see page 160)
- [Configure Custom Provisioning Process in CA Process Automation](#) (see page 163)
- [Disable Default CA Service Catalog Rules](#) (see page 165)
- [Configure Touchpoint in CA Server Automation](#) (see page 167)
- [Configure Network in CA Server Automation](#) (see page 170)
- [Configure CA Automation Suite for Clouds Foundation](#) (see page 172)
- [Integrate CA Process Automation with CA Server Automation](#) (see page 188)
- [Configure CA Automation Suite for Clouds Base Configuration for ESX](#) (see page 189)
- [Integrate CA Business Intelligence with CA Service Catalog](#) (see page 234)
- [Integrate CA Business Intelligence with Active Directory](#) (see page 251)
- [Configure CA IT Client Manager Software Delivery](#) (see page 257)
- [CA IT Client Manager Installation and Configuration](#) (see page 262)

Integrate CA Service Catalog with CA Server Automation

CA Automation Suite for Clouds Base Configuration consists of multiple components that are integrated and loaded with prebuilt content. The following steps walk you through integrating and loading the prebuilt content, bringing the CA Automation Suite for Clouds Base Configuration together.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator (spadmin).
2. Click Administration, Configuration.
3. Click CA Automation Suites Reservation Manager.

Options	CA Automation Suites Reservation Manager		
	Property	Value	Modify
CA API Web Services	Enable HTTPS	Yes	
CA Automation Suites Reservation Manager	Host Name	ASC-SA	
CA Business Intelligence(CA BI)	Port Number (1-65535)	443	
CA Business Service Insight	UI Port Number (1-65535)	8443	
CA CMDB	User ID	ASCapAdmin	
CA CMDB Visualizer	User Password	*****	
CA Process Automation			
CA Service Desk			
CA Workflow			
Event Manager			
File Store Information			
Mail Server			
Portal			
Request SLA			
Role Manager			
Server Information			
Single Sign On Authentication			
System Information			
User Default			

4. Click Modify and update the following property values, as appropriate:

Enable HTTPS

Yes

Host Name

Enter the hostname of the server where Reservation Manager is installed.

Port Number

443

UI Port Number

8443

User ID

Enter the CA Server Automation Administrator.

User Password

Enter the password for the CA Server Automation Administrator.

5. Click Test in the upper right corner to validate the integration.
A success message opens.
6. Click OK.
7. Click Launch in the upper right corner and validate that you can log in to Reservation Manager.
8. Close Reservation Manager.

CA Service Catalog is integrated with CA Server Automation.

Integrate CA Service Catalog with CA Process Automation

Complete the following procedure to integrate CA Service Catalog with CA Process Automation.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.
2. Click Administration, Configuration.

3. Click CA Process Automation.

CA Process Automation Configurations		Launch	Load	Configure	Test
Order of configuration: Load > Configure > Test					
▲ CA Process Automation * (itpam)					
Property ^	Value				
Certificate File Path on CA Process Automation	Not Configured				
Enable Automatic Retry	Yes				
Enable HTTPS	No				
Host Name					
Key File Path on CA Process Automation	Not Configured				
Password for Certificate on CA Process Automation	Not Configured				
PEM Certificate File Name	ITPAMCertfile.pem				
Port Number (1-65535)	8080				
Retry Count (0-10)	3				
Retry Interval (0-3600) (in secs.)	15				
Use Certificate for Authentication	No				
User ID	pamadmin				
User Password	*****				

4. Modify the following property values, as appropriate:

Enable Automatic Retry

Yes

Enable HTTPS

No

Host Name

Enter the host name of the server where CA Process Automation is installed.

PEM Certificate File Name

Accept the default value or leave the field blank.

Port Number (1-65535)

8080 (default) unless it was changed due to a port conflict.

Retry Count (0-10)

3 (default)

Retry Interval (0-3600) (in secs.)

15 (default)

User Certificate for Authentication

No

User ID

Enter the CA Process Automation Administrator (PAMadmin).

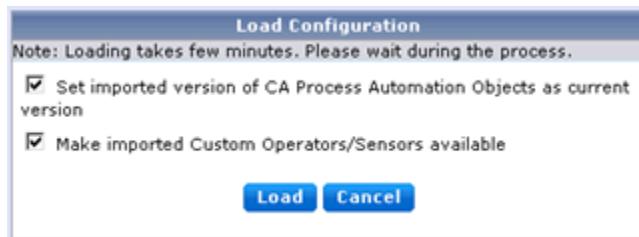
User Password

Enter the password for the CA Process Automation Administrator.

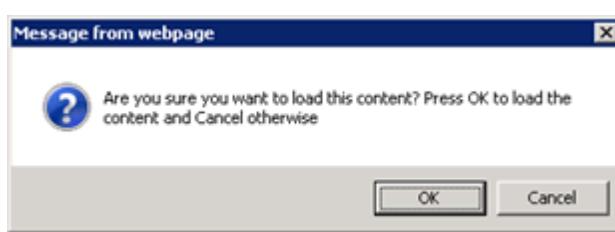
5. Click Launch in the upper right corner and validate that you can log in to the CA Process Automation web client.

Note: The CA Server Automation Custom Operator is loaded during the CA Server Automation installation when you integrated CA Process Automation with CA Server Automation.

6. Close the CA Process Automation web client.
7. Click Load in the upper right corner.



8. Complete the following settings:
 - Select Set imported version of CA Process Automation Objects as current version.
 - Select Make imported Custom Operators/Sensors available.
9. Click Load.



10. Click OK.



11. Click OK, when the content has successfully loaded.
12. Click Configure in the upper right corner.



13. Click OK.
14. Click Launch again and log in to CA Process Automation web client.
15. Click the Library tab.
16. Confirm the following details:
 - Confirm that the CA SDM and CA SLCM folders were added.
 - Confirm under Custom Operators the CA SDM and CA SLCM have been added.
17. Click the CA SLCM folder.
Note: Delete all the unwanted or unused dataset values to ensure proper connection.
18. Double-click SLCM_GlobalDataset, and click Check Out.
19. Click Login Parameters_CHANGE ME and enter the following details:
password
Specifies the CA Service Catalog Administrator password

20. Repeat step 12 for configuration changes to take effect.

Note: All other parameters except the password are populated when you configure CA Service Catalog with CA Process Automation and click the Configure button.

21. Click APP URLs CHANGE ME, verify the following fields, and save the changes:

SLCM_URL

Specifies CA Service Catalog URL.

ITPAM_URL

Specifies CA Process Automation URL.

22. Click Misc Parameters CHANGE ME and complete the following details:

Administrator

Specifies the CA Service Catalog Administrator user name (spadmin).

If a Mail Server is configured, enter the Administrator_Email and EmailFromAddress.

23. Click Save, and then Check In the changes.
24. Log in to CA Service Catalog.
25. Click Administrator, Configuration, CA Process Automation.
26. Click Test in the upper right corner for validating the integration.
27. Click OK, when the connection successful message appears.

More Information:

See [Configure SLCM_GlobalDataset](#) (see page 179).

Update Load Balancer Details

If CA Service Catalog is running in a clustered environment, update the SLCM global dataset in CA Process Automation with the load balancer details.

Follow these steps:

1. Log in to the CA Process Automation console as the CA Process Automation Administrator.
2. Click the Library tab.
3. Click the root folder (/), CA SLCM.
4. Double-click SLCM_GlobalDataset, and click Check Out.

Note: Delete all the unwanted or unused dataset values to ensure proper connection.

5. Click APP URLs Change ME and enter the following details:

SLCM_URL

Specifies CA Service Catalog URL.

6. Click Save and then Check In the changes.
7. Close the SLCM_GlobalDataset form.

Configure CA Process Automation with Active Directory Server

Verify the following items before configuring the Active Directory server:

- Configure the Active Directory server with SSL and export the certificate into CA Process Automation.
- [Set up CA Process Automation with the SSL configuration and install the Active Directory certificate](#) (see page 161).
- [Verify that the LDAP module is configured with SSL value for the Security Protocol](#) (see page 163).

Add an SSL Certificate to CA Process Automation

Follow these steps:

1. Do one of the following to retrieve the certificate file from the Active Directory server.

For the instance to establish an SSL connection between CA Process Automation and an Active Directory server, retrieve the certificate.

- Log in to `http://i.p./certsrv` and download the certificate.

i.p.

Defines the IP address of the Active Directory server.

- Log in to the Active Directory server and import the certificate directly.

2. Copy the certificate file to the computer where the CA Process Automation LDAP module is running.

3. Import the certificate using the following keytool command:

```
keytool -import -alias PAM -file certnew.cer -keystore  
"C:\\\\Program Files\\\\Java\\\\  
jdk1.7.0_51\\\\jre\\\\lib\\\\security\\\\cacerts"
```

Where `certnew.cer` is the path to the certificate file retrieved in step 1.

`C:\\\\Program Files\\\\Java\\\\ jdk1.7.0_51\\\\jre\\\\lib\\\\security\\\\cacerts` is the path to the cacerts file within the Java JRE or JDK.

Note: Update the JDK path depending on the JDK version you install. For example, use `jdk1.7.0_51` in the path if you installed JDK version `1.7.0_51`.

- The keytool program is part of the Java installation.
- The Keytool prompts for a password. The password is `changeit` by default.
- The Keytool prompts whether to 'Trust this certificate?[no]'. Enter yes.

4. Add the following lines in the CA Process Automation file:

PAM\server\c2o\bin\c2osvcw.conf

(or in the case of an upgrade): I

PAM_DIR%\server\c2o\bin\c2osvcw.conf:

```
wrapper.java.additional.11=-Djavax.net.ssl.trustStore="C:\\Program Files\\Java\\ jdk1.7.0_51\\jre\\lib\\security\\cacerts"  
wrapper.java.additional.12=-Djavax.net.ssl.trustStorePassword  
="changeit"
```

The numbers could be different for you. Start with the next available number. If wrapper.java.additional.11 is already defined, use 12 and 13.

The program folder is different for your JDK installation.

The password is changeit.

5. Restart the CA Process Automation Server.

Set Up the Active Directory Server

To establish an SSL connection between the CA Process Automation-LDAP Module and an Active Directory server, verify that the Active Directory server is set up:

1. The Certificate Services are installed on your Active Directory server (consult your Active Directory administrator for this task).
2. The Automatic Certificate Request is configured for Domain Controllers (consult your Active Directory administrator for this task).

Note: You cannot create or modify an existing user account password in Active Directory unless CA Process Automation is connected to the Active Directory server through the SSL.

Configure CA Process Automation for ssl

Follow these steps:

1. Open and log in to the CA Process Automation web client.
2. Click the Configuration tab.
3. Select Domain from the left pane in the Browser window.
This step activates the toolbar buttons.
4. Select the Modules tab.
5. Select Directory Services and select Lock in the padlock icon to edit the parameter.
6. Double-click the Directory Services module.
7. Enter the value `ssl` in the Security Protocol field.
Important! Make sure to enter `ssl` in lower case.
8. Click Save and Close.
9. Click Unlock, Save in the padlock toolbar.
10. Close the CA Process Automation Client and the CA Process Automation Orchestrator.
11. Open Services and restart the CA Process Automation Service.

Configure Custom Provisioning Process in CA Process Automation

As an administrator you can configure preprovisioning and post-provisioning processes.

The preprovisioning processes must not create the virtual machine reservation itself. You can verify the resource availability, set up the environment before the reservation is created, and so on. The postprovisioning processes must not complete the request itself. The reservation is fulfilled by the event receiver when all the postprovisioning processes are completed.

Follow these steps:

1. Log in to CA Process Automation as an administrator.
2. Click Library, CA ASC Base Console.
3. Double-click ASC_Global Dataset.
4. Click Check Out to edit the parameters.

Note: Delete all the unwanted or unused dataset values to ensure proper connection.

5. Expand the ServerAuto parameters, ServiceMappings.
6. Expand the Parameters 0 or 1.
 - 0 for Reserve VM.
 - 1 for Reserve using Template.

Two sections display, which allows you to configure pre-execution and post-execution processes.

Expand a parameter, you can see different properties like ServiceType, ServiceName, HyperVisor, PostExecution and PreExecution.

7. Right-click the PostExecution or PreExecution and select Add indexed Value.

A new row is added.
8. Double-click the value field in the new row.
9. Select the process you want to link to preprovisioning or postprovisioning process.
10. Click OK, Save, and Check In.
11. Repeat the steps 7 to 10 to add more processes for provisioning a virtual machine.

You have configured custom processes to execute with the provisioning a virtual machine.

Disable Default CA Service Catalog Rules

If you are already using any of the following default CA Service Catalog rules in your environment, we recommend disabling them. Default rules create conflict with the CA Automation Suite for Clouds content whenever a request is raised. Additionally, if you have created custom actions for the default CA Service Catalog rules, add the actions again to the new set of rules.

Important! The content pack includes equivalent rules for the set of the following rules by adding a condition that does not conflict with the non-ASC content.

The content pack includes variants for all the conflicting default CA Service Catalog rules. The rules are separated in two groups with the prefix ASC and NON-ASC, and they are enabled by default. You can enable or disable the rules with the prefix NON-ASC after deploying and configuring the content packs.

The following tables list the rules that are modified:

These rules are located under Request/Subscription Item Change (Administration->Events-Rules-Actions).

Rules to be Disabled	Equivalent Rules CA Automation Suite for Clouds Release 1.7.1 Provides
When Status is Submitted and Approval Process is driven by Workflow.	NON-ASC- When Status is Submitted and Approval Process is driven by Workflow.
When Status is Submitted and Approval Process is driven by Policy	NON-ASC- When Status is Submitted and Approval Process is driven by Policy.
When Status is Pending Approval and Requested By and Requested For users are different.	NON-ASC- When Status is Pending Approval and Requested By and Requested For users are different.
When Status is Pending Approval.	NON-ASC- When Status is Pending Approval.

[Disable Default CA Service Catalog Rules](#)

Rules to be Disabled	Equivalent Rules CA Automation Suite for Clouds Release 1.7.1 Provides
When Status is Fulfillment Canceled.	NON-ASC- When Status is Fulfillment Canceled.
When Status is Pending Fulfillment.	ASC-FC-GENERIC-When Status is Pending Fulfillment and not ASC

These rules are located under Request Pending Action Change (Administration > Events-Rules).

Rules to be Disabled	Equivalent Rules CA Automation Suite for Clouds Release 1.7.1 Provides
When action is Cancelled.	NON-ASC - When action is Canceled.
When action is Delegated.	NON-ASC - When action is Delegated.
When action is Returned.	NON-ASC - When action is Returned.
When action is Taken.	NON-ASC - When action is Taken.
When action is Transferred	NON-ASC - When action is Transferred.
When Fulfilled.	NON-ASC - When Fulfilled.
When Pending Approval actions are Assigned.	NON-ASC - When Pending Approval actions are Assigned.
When Pending Approval actions are Assigned and Requested By and Requested For users are different.	NON-ASC - When Pending Approval actions are Assigned and Requested By and Requested For users are different.
When Pending Fulfillment actions are Completed.	NON-ASC - When Pending Fulfillment actions are Completed.
When Status is Approved.	NON-ASC - When Status is Approved.
When Status is Rejected.	NON-ASC - When Status is Rejected.
When Pending Fulfillment actions are Assigned.	NON-ASC - When Pending Fulfillment actions are Assigned.

Configure Touchpoint in CA Server Automation

Perform the following procedure to configure a touchpoint that is required for creating the datastore. This procedure requires you to first install the CA Process Automation agent on the CA Server Automation server, and then configure the touchpoint.

Follow these steps:

1. Log in to the CA Server Automation server.
2. Open a web browser and launch CA Process Automation client.
3. Log in as CA Process Automation Administrator (pamadmin).
4. Click the Configuration tab.
5. Click the Installation palette.
6. Click Install for Install Agent
7. At the File Download prompt, click Run to start the installer. If you receive a security warning, click Run.

The Language Selection dialog opens. The language of the host computer is selected by default.

8. Click OK or select another language and click OK.

The welcome page of the CA Process Automation Agent Setup wizard appears.

9. Click Next.

The License Agreement opens.

10. Read the license. If you accept the terms, click I accept the terms of the License Agreement. Click Next.

The Set Java Home Directory page opens.

11. If the displayed Java home directory is not correct, browse to the JRE folder.

The default JRE folder for Windows follows, where jre has a release-specific name:

C:\Program Files\Java\jre

12. Click Next.

The Select Destination Directory page opens. The default path follows:

C:\Program Files\CA\PAM Agent

13. Click Next to accept the default or enter a destination directory for the new agent, and click Next.

The Select Start Menu Folder page opens.

14. (Windows only) Click Next to accept CA Process Automation Agent as your Start menu shortcut or type a new name.

15. (Optional) Create short cuts for all users on this host.

16. (Optional) Do not create Start menu Folder.

17. Click Next

18. Examine the Domain URL and the URL of the Domain Orchestrator from which you launched the agent installation. Click Next.

19. Complete the General Properties page as follows:

a. Accept the Agent Host name entry. This name identifies the host from which you started the installation.

b. Change or accept the default Display Name, the host name.

c. Accept 7003 as the Agent Port unless this port is used. Alternatively, enter another port number such as 57003.

d. If you launched the agent installation from a Windows host, select Install as Windows Service.

e. (Optional) Select Start Agent After Installation.

Starting the agent lets you view the active agent and continue with the agent configuration.

20. Click Next to accept the default temporary directory for executing scripts or enter another path and then click Next.

Note: An acceptable path contains no spaces.

The Set PowerShell execution policy page opens.

21. Read the displayed explanation and complete the setting in one of the following ways.

- If you use Windows PowerShell, select the Set PowerShell Execution Policy to set the PowerShell execution policy and browse to the PowerShell host location and click Next.

This setting enables you to run Windows PowerShell scripts through this agent.

- If you do not use Windows PowerShell, click Next.

The CA Process Automation agent installation begins.

22. Click Finish.

23. Start the agent service. Click Start, Programs, CA, *agent-name*, Start agent service.

24. Click the Configuration Browser palette on the Configuration tab.

25. Click Refresh.

26. Expand Agents and verify that your agent name is listed.

Continue configuring touchpoint in CA Process Automation.

27. Expand Configuration.

28. Click the Configuration Browser palette.

29. Expand Domain.

30. Right-click Default Environment, and select Lock.

31. Expand Agents, right-click the agent name, select Configure touchpoint at, Default Environment.

The Add Agent Touchpoint popup appears.

32. Enter the name of the touchpoint and click OK.

The newly added touchpoint appears under All Touchpoints, under Domain, Default Environment.

33. Click Save.

34. Right-click Default Environment, and select Unlock.

You have configured the touchpoint on the CA Server Automation server.

Configure Network in CA Server Automation

You can configure a network and can associate it with the IP addresses. You can also specify how to assign the IP address to systems requestor by using DHCP server or static IPs. You can also set up servers that must be included in the network.

Allocation of Static and Dynamic IP schemes

The network pools can be configured to allocate static and dynamic IP schemes. A service consumer can select any IP while provisioning a virtual machine. If the template has multiple network interfaces, each network interface can be configured to a different IP scheme by selecting the desired network pool.

Allocation of Good and Low Quality Network

You can create various network pools and can associate them with different VLANs in the VCenter. The network pools can be configured to a good quality network and a low quality network.

Follow these steps:

1. Log in to CA Server Automation as an administrator.
2. Click Management, Manage, Manage Networks.
3. Click + to add network details.

A form opens.

4. Complete the following information in the Network Address Pool Properties tab and click Next.
5. Complete the information in the DNS/WINS/Domain tab and click Next.
6. Complete the information in the IP Pools tab.
 - a. Select Require DNS Entries for Static IP Address, to assign a static IP address for DNS.
 - b. Click + to add a range of IP addresses for the IP Pool and select the pool type.
 - c. Click OK.
 - d. Click Next.
7. Complete the information in the Port Groups tab.
 - a. Click + to add Port Groups to the network.
 - b. Select the Pool Groups.
 - c. Click Add.
8. Click Finish.

The VLAN is added to the network pool.

Configure Network Pool Access to Organizational Units

As a Service Delivery Administrator you can associate the network pools and organizational units. This association enables the end users from the organization to access virtual machines in the network pool.

Follow these steps:

1. Log in to the Reservation Manager using the CA Server Automation administrator user credentials and the following URL:
`https://servername:port/ssrm`
See your [Installation Worksheet](#) (see page 19) for the values.
2. Click Administer your Reservation Manager, Manage your Organizational Units.

3. Select the organization for which you want to provide the network access.

Example: Development

4. Click the Network Access tab.
5. Add or remove the networks from the Available Networks to Selected Networks using the arrows.
6. Click OK.

You have configured network pool access to all users of an organizational unit. The end users can use the network when provisioning a virtual machine.

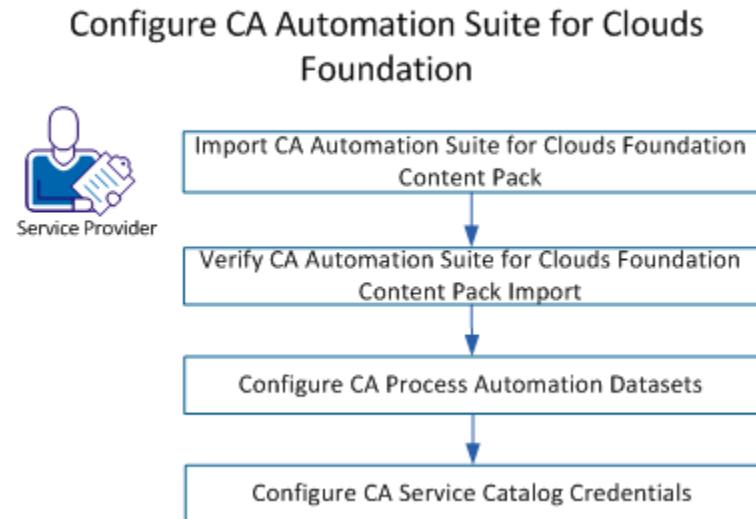
Configure CA Automation Suite for Clouds Foundation

The CA Automation Suite for Clouds Base Configuration is a content pack containing a combination of the following items:

- CA Service Catalog Form Objects
- CA Service Catalog Service Offerings
- CA Service Catalog Rule Objects
- CA Process Automation Workflows
- Report Data Objects
- Images
- JavaScript Files

Important! Install the solution in the order that is specified in the following process, because installations and configurations are cross-dependent. CA Technologies does not support deviations from the installation and configurations, except when specified. These procedures also assume that you have the required infrastructure and non-CA Technologies software installed.

The following diagram illustrates how a Service Provider configures the components of CA Automation Suite for Clouds Foundation:



Follow these steps:

1. [Import CA Automation Suite for Clouds Foundation Content Pack](#) (see page 174).
2. [Verify CA Automation Suite for Clouds Foundation Content Pack Import](#) (see page 176).
3. [Configure CA Process Automation Datasets](#) (see page 179).
4. [Configure CA Service Catalog Credentials](#) (see page 184).

Import CA Automation Suite for Clouds Foundation Content Pack

Verify that all configuration steps are performed before deploying the CA Automation Suite for Clouds Base Configuration.

Follow these steps:

1. Unzip CA_ASC_Foundation.zip contents from the media to the %USM_HOME%/filestore/contentpacks folder.
2. Open a CA Service Catalog Command Prompt window, change directory to: %USM_HOME%/filestore/contentpacks/CA ASC Foundation.
3. Copy the securityrealm folder that is under the CA ASC Foundation to the CA Process Automation server.
4. Run *DeployBaseConsole.cmd*.
5. Type the tenant ID at the following prompt, and press Enter:
[input] Enter the id of the tenant you want to import the content pack into (Required):
Note: The tenant ID is case-sensitive.
For example, Forward Inc.
6. Type y at the following prompt to proceed with the deployment:
Installation will re-start CA Service Catalog multiple times.
Please press y to continue or any key to exit:
7. Press Enter at the following prompt:
Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance
[INSTALLED_DEFAULT]
On successful deployment, the BUILD SUCCESSFUL message opens.
8. Complete the details to configure the database credentials of ASC schema at the following prompts:
Enter Service Catalog Database Administrator (Default sa):
Enter Service Catalog Database Administrator Password:

9. Type **y** at the following prompt to proceed creating groups:

If the build is successful, press **y** to Create Groups or any key to exit the setup.

10. Complete the following details about CA Service Catalog, if prompted:

Enter Service Catalog Host Name (Default localhost):

Enter Service Catalog Port Number (Default 8080):

Enter Service Catalog Admin User ID:

Enter Service Catalog Admin Password:

The installer validates the CA Service Catalog credentials and prompts for the CA EEM details.

11. Complete the following details for creating groups in CA EEM:

Enter EEM Admin User ID (Default eiamadmin):

Enter EEM Admin Password

After the groups are created, the following message opens:

Offering permissions set successfully in CA Service Catalog.

The following groups are created in CA EEM and assigns permissions to the service offerings in CA Service Catalog as defined in the content pack groups properties file:

- ASCgrp_baseconsole_NormalUser
- ASCgrp_baseconsole_Admin

For more information, see the %USM_HOME%/filestore\contentpacks\CA ASC Foundation\prescripts\group_service.properties file.

Configuring Content Pack in a Clustered Mode

Perform more steps on all nodes, for installing cartridges that are configured in a clustered mode. Typically, the installation is performed on a single node and contents like services, forms, events, and reports are reflected on all nodes. However, files like plugin jars, requestshared.xml, must be copied manually to all the other nodes of the cluster.

Follow these steps:

1. Extract *cartridge-name.zip* to the %USM_HOME%\filestore\content-packs\ and open the cartridge-name folder.
2. Open the prescripts folder and run the cartridge-name prescript.bat file as an Administrator.
3. Copy the contents of the following folders:
 - plugins folder to the %USM_HOME%\filestore\plugins folder.
 - images\offerings folder to the %USM_HOME%\filestore\images\offerings folder.
 - images\rateplans folder to the %USM_HOME%\filestore\images\rateplans folder.
4. Restart the CA Service Catalog service on the Node.

Verify CA Automation Suite for Clouds Foundation Content Import

After you complete the import, verify that the import is successful.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration.
3. Click Content Packs in the left-side menu, and select the content pack that you imported.

4. Verify the following steps:

- The Content Pack Details section lists the details that you specified when you created the content pack.

Name

Displays the name of the content pack.

Example: CA ASC Foundation

Description

Displays the description of the content pack.

Example: This content pack helps create new users in Active Directory and manage them. The content pack also helps in assigning permissions to various service offerings.

Version

Displays the version of the content pack.

Example: 1.7.1

Author

Displays the author name.

Example: CA Technologies

Status

Displays the status of the content pack.

Example: Enabled

Id

Displays the unique ID of the content pack.

Example: CA_ASC_FC_v1.7.1_en

Note: Compare the information with that contained in the contentpack.properties file. This file is created during the import of the content package.

- The Content section lists the objects that are specified according to the criteria selected on the import. The Objects are as follows:
 - Offerings (Services)
 - Service Option Groups
 - Forms
 - Events (rules, Rule Actions)
 - Report Data Objects
 - Report Variables
- 5. (Optional) If you have to create an inherited copy of any services through the Service Builder, select *one* of the following options:
Note: This selection cannot be reverted.
 - Click OK to copy all of the associated Service Option Groups.
 - Click Cancel to copy only Services and link to the original Service Option groups.

Configure Default Cancellation State

By default, when you uninstall a service cartridge, the status of all requests change to Pending Cancellation. This state prevents you from closing any open requests after uninstall. So you change the default cancellation state to Cancel.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Accounting, Configuration.
3. Select Subscription Configuration from the Options menu.
4. Modify *Default Cancellation State* to Cancel.
5. Click Update Configuration.

You have changed the default cancellation state.

Configure CA Process Automation Datasets

Datasets define variables and store data in CA Process Automation.

Configure SLCM_GlobalDataset

SLCM global dataset is used for the communication between CA Service Catalog and CA Process Automation. See the [Integrate CA Service Catalog with CA Process Automation](#) (see page 155) section for detailed procedure to configure SLCM_GlobalDataset.

Configure ASC_Security_GlobalDataset

Follow these steps:

1. Log in to CA Process Automation web client as the CA Process Automation Administrator.
2. Click the Library tab, CA ASC Base Console.
3. Double-click ASC_Security_GlobalDataset, and click Check Out.
4. Click Login Parameters_CHANGE ME and type the following details:

userID

Specifies the CA Service Catalog Administrator user name (spadmin)

password

Specifies the CA Service Catalog Administrator password

businessUnit

Specifies the CA Service Catalog Business Unit (This value is case-sensitive).

For example, Forward Inc.

5. Click APP URLs CHANGE ME, verify the following fields, and save the changes:

SLCM_URL

Specifies CA Service Catalog URL.

ITPAM_URL

Specifies CA Process Automation URL.

6. Click Misc_Parameters_CHANGE ME, verify the following fields, and save the changes:

Administrator_Email

Specifies the Administrator email.

7. Click AD Parameters CHANGE ME

ldaphost

Specifies the Active Directory Host Name.

ldapuser

Specifies the Active Directory administrator user name

ldapport

Specifies the Active Directory SSL Port.

Default: 636

Idappassword

Specifies the AD administrator password.

basedn

Specifies the Base DN.

Example: DC=mydomain, DC=com

userprefix

Specifies the User Prefix.

Default: cn

basednprefix

Specifies the Base DN Prefix. Default CN=Users.

adminbasednprefix

Specifies the Admin Base DN Prefix. Default CN=Users.

8. Click EEM Parameters and type the following details:

eemhost

Specifies the FQDN of CA EEM host name where CA Service Catalog is registered.

eemuser

Specifies the CA EEM administrator user name (Eiamadmin).

eempassword

Specifies the CA EEM administrator password.

eemApplication

Specifies the application name that is registered with CA EEM for CA Service Catalog.

pamPath

Specifies the file path of the *SecurityRealm* folder on the CA Process Automation server.

Note: Unzip the securityrealm.zip from the %USM_HOME%/filestore/contentpacks/CA ASC Foundation/securityrealm and copy to the securityrealm folder to the CA Process Automation computer.

9. Click Save, and then Check In the changes.

Configure ASC_GlobalDataset

Follow these steps:

1. Log in to the CA Process Automation web client.
2. Click Library tab.
3. Click the CA ASC Base Console folder.
4. Double-click ASC_GlobalDataset, and click Check Out.

Note: Delete all the unwanted or unused dataset values to ensure proper connection.

5. Expand *Error Handling Parameters* and then update the following information:

globalCancelFlag

Specifies the global cancel flag status.

This flag takes the precedence over the cancelFlag. If this value is true, you can skip reviewing cancelFlag status.

cancelFlag

Specifies the cancel flag status.

This flag is specific to the current cartridge. In this case, CA Automation Suite for Clouds Foundation Console.

sendToUser

Specifies whether to notify the users when an error occurs.

maxRetryCount

Specifies the number of retries that you want to set for a service request.

adminGroup

Defines the administrator group to which the requests are assigned when an error occurs. Separate each entry with a semicolon.

retryinterval

Specifies the time interval in seconds between each retry.

invalidsession

Specifies that an error message must be displayed when a session is invalid.

6. Click ErrorMessages page.

This page lists custom handling for specific errors. If any error messages need to be handled, then add an indexed value to the array.

7. Expand index[0] and parameters, and complete the following details:

searchString

Specifies the string to identify error message.

exceptionMessage

Specifies the actual exception or error message.

cancelRequest

Specifies the whether to cancel the request or not.

Default: False

sendToUser

Specifies whether to send email to user or not.

Default: False

8. Click Save, Check In.

Configure CA Service Catalog Credentials

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, Content Configuration.
3. Click CA Embedded Entitlements Manager.

● =Required

△ CA Embedded Entitlements Manager

● Host Name:

● Port Number (1-65535):

● EEM Username:

● EEM Password:

Enable HTTPS:

Launch

4. Complete the following details:
 - Enter the Host Name of the server where CA EEM is installed
 - Enter the Port Number for CA EEM
Value: 5250
 - Enter EEM User Name(Eiamadmin)
 - Enter EEM Password
 - Verify that Enable HTTPS is checked.
5. Click Launch and log in to CA EEM and verify that the configuration is correct.
6. Close CA EEM.
7. Click Save.
8. Click OK for the confirmation.
9. Click CA Process Automation.

The screenshot shows a configuration dialog box for the CA IT Process Automation Manager. It has a title bar with the text 'CA IT Process Automation Manager'. Below the title, there are three required fields marked with red asterisks: 'Host Name' (input field), 'Port Number (1-65535)' (input field), and 'Enable HTTPS' (checkbox). At the bottom of the dialog is a blue 'Launch' button.

10. Complete the following details:
 - Enter the Host Name of the server where CA Process Automation is installed.
 - Enter the Port Number for CA Process Automation.
Value: 8080
 - Verify that Enable HTTPS is not checked.
11. Click Launch and log in to CA Process Automation and verify that the configuration is correct.
12. Close CA Process Automation.
13. Click Save.
14. Click OK to confirm.

15. Click CA SLCM Configuration.

• = Required

△ SLCM Properties

- SLCM Host Name:
- SLCM Port Number:
- SLCM Username:
- SLCM Password:

16. Complete the following details:

- Enter the SLCM Host Name of the server where CA Service Catalog is installed.
- Enter the SLCM Port Number for CA Service Catalog.
Value: 8080
- Enter the CA Service Catalog Administrator user name in the SLCM Username field.
Value: spadmin
- Enter the password for the CA Service Catalog Administrator in the SLCM Password field.

17. Click Save.

18. Click OK for the confirmation.

19. Click CA Spectrum Automation Manager.

• = Required

△ CA Spectrum Automation Manager

- Host Name:
- Port Number (1-65535):

Enable HTTPS:

Launch

20. Complete the following details:
 - Enter the Host Name of the server where CA Server Automation is installed.
 - Enter the Port Number for CA Server Automation.
Value: 8443
 - Verify that Enable HTTPS is checked.
21. Click Launch and log in to CA Server Automation and verify that the configuration is correct.
22. Close CA Spectrum Automation Manager.
23. Click Save.
24. Click OK for the confirmation.
25. Click CA Spectrum Reservation Manager.

The screenshot shows a configuration dialog for the CA Spectrum Reservation Manager. It includes a required field for the Host Name and a port number field (1-65535). The 'Enable HTTPS' checkbox is checked. A 'Launch' button is at the bottom.

26. Complete the following details:
 - Enter the Host Name of the server where Reservation Manager is installed.
 - Enter the Port Number for Reservation Manager.
Value: 8443
 - Verify that Enable HTTPS is checked.
27. Click Launch and log in to Reservation Manager and verify that the configuration is correct.
28. Close CA Spectrum Reservation Manager.
29. Click Save.
30. Click OK to confirm.
31. Close CA Service Catalog.

The CA Service Catalog configuration is complete.

Integrate CA Process Automation with CA Server Automation

When an event like completion of provisioning a machine occurs, a CA Process Automation process is triggered to alert users to completion of the task. If such integration is not in place, the user must verify task completion manually.

Follow these steps:

1. Log in to CA Server Automation as administrator (default username: sys_service).

Sample URL: <CA Server Auto hostname>: CA Portal/UI

2. Click Administration, Configuration, CA Process Automation Server.
3. Complete the following information:

Server Name

Specifies the server on which CA Process Automation is installed.

User Name

Specifies the CA Process Automation administrator user name.

Password

Specifies CA Process Automation log in password.

Port

Specifies the port number of the server on which CA Process Automation is installed.

Protocol

Specifies the CA Process Automation server protocol.

Connection Status

Displays the connection status.

4. Click Action, Validate to test the connection.

The connection status is verified and displayed.

5. Click Action, Save.

The CA Process Automation configuration is complete.

Configure CA Automation Suite for Clouds Base Configuration for ESX

The CA Automation Suite for Clouds Base Configuration for ESX is a content pack containing a combination of the following items:

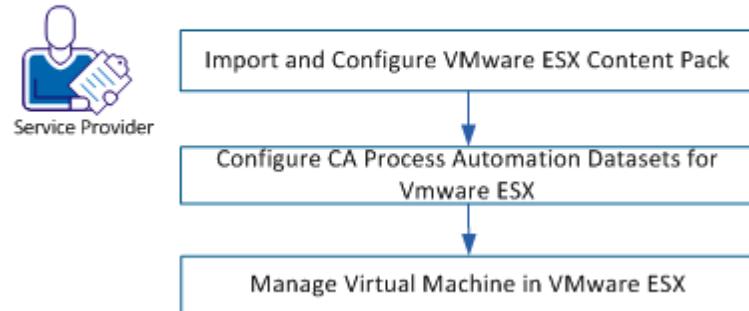
- CA Service Catalog Form Objects
- CA Service Catalog Service Offerings
- CA Service Catalog Rule Objects
- CA Process Automation Workflows
- CA Server Automation Rules
- CA Server Automation Actions
- Report Data Objects
- Images
- JavaScript Files

Important! Install the solution in the order that is specified in the following process, because installations and configurations are cross-dependent. CA Technologies does not support deviations from the installation and configurations, except when specified. These procedures also assume that you have the required infrastructure and non-CA Technologies software installed.

[Configure CA Automation Suite for Clouds Base Configuration for ESX](#)

The following graphic illustrates how a service provider configures the CA Automation Suite for Clouds Base Configuration for VMware ESX:

Configure CA Automation Suite for Clouds Base Configuration for VMware ESX



Perform the following steps:

1. [Import and Configure VMware ESX Content Pack](#) (see page 191).
2. [Configure CA Process Automation Datasets for VMware ESX](#) (see page 199).
3. [Managing Virtual Machines in VMware ESX](#) (see page 208).

Import CA Automation Suite for Clouds Base Configuration for ESX Content Pack

You import the CA Automation Suite for Clouds Base Configuration ESX content pack in to CA Service Catalog to make the ESX available to your Service Consumers. For more information about services, see the CA Service Catalog documentation.

Important! The ESX package is delivered with the updated *requestshared.xml* file. This XML file replaces the existing *requestshared.xml* file at the location `%USM_HOME%\view\webapps\usm\locale\jcusen\request\`. The existing file is backed up with the name *requestsharedBKP.xml*.

If you introduced any custom states to the CA Service Catalog through the existing *requestshared.xml*, copy these nodes to the new *requestshared.xml* file.

Follow these steps:

1. Unzip the *CA ASC Server Automation - ESX.zip* file to the `%USM_HOME%\filestore\contentpacks` folder on the CA Service Catalog server.

Note: Record the location for the reference in the [Installation Worksheet](#) (see page 19).

2. Run *DeployServerAutomation-ESX.cmd*.

The content pack deployment starts automatically.

3. Type the tenant id at the following prompt, and press Enter:
[input] Enter the id of the tenant you want to import the content pack into (Required):

Note: The tenant ID is case-sensitive.

For example, Forward Inc.

4. Type *y* at the following prompt to proceed with the deployment:

Installation will re-start CA Service View multiple times.
Please press *y* to continue or any key to exit:

5. Press enter at the following prompt:

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

Follow the onscreen instructions. On the successful deployment, the BUILD SUCCESSFUL message appears. The chargeback feature installation starts.

6. Type y at the following prompt to proceed creating groups:

If build is successful, enter y to Create Groups or any key to exit the setup:

After the groups are created, the following message opens:

Offering permissions set successfully in CA Service Catalog.

The following groups are created in CA EEM and assigns permissions to the service offerings in CA Service Catalog as defined in the content pack groups properties file:

- ASCgrp_sa_esx_Reservation_Create
- ASCgrp_sa_esx_DataStore
- ASCgrp_sa_esx_Reservation_Change
- ASCgrp_sa_esx_Reservation_Return
- ASCgrp_sa_esx_Power_Functions
- ASCgrp_sa_esx_Snapshots
- ASCgrp_sa_esx_Reservation_Extend
- ASCgrp_sa_esx_offering_admin

Configuring Content Pack in a Clustered Mode

Perform more steps on all nodes, for installing cartridges that are configured in a clustered mode. Typically, the installation is performed on a single node and contents like services, forms, events, and reports are reflected on all nodes. However, files like plugin jars, requestshared.xml, must be copied manually to all the other nodes of the cluster.

Follow these steps:

1. Extract *cartridge-name.zip* to the %USM_HOME%\filestore\content-packs\ and open the *cartridge-name* folder.
2. Open the *prescripts* folder and run the *cartridge-name* *prescript.bat* file as an Administrator.
3. Copy the contents of the following folders:
 - *plugins* folder to the %USM_HOME%\filestore\plugins folder.
 - *images\offerings* folder to the %USM_HOME%\filestore\images\offerings folder.
 - *images\rateplans* folder to the %USM_HOME%\filestore\images\rateplans folder.

Restart the CA Service Catalog service on the Node.

Verify ESX Content Pack Import

After you have completed the ESX content package import, you verify that the import was successful. In addition, you verify if the chargeback services are available.

Follow these steps:

1. Log in to CA Service Catalog as an administrator and select Catalog, Configuration.
2. Click Content Packs in the left menu and select the content pack that you imported.

3. Verify the following details:

- The Content Pack Details section lists the details of the content pack.

Name

Displays the name of the content pack.

Example: CA ASC Server Automation - ESX

Description

Displays the description of the content pack.

Example: This content pack provides Cloud reservation and snapshot services to ESX through Server Automation.

Version

Displays the version of the content pack.

Example: 1.7.1

Author

Displays the author name.

Example: CA Technologies

Status

Displays the status of the content pack.

Example: Enabled

Id

Displays the unique ID of the content pack.

Example: CA_ASC_SA_ESX_v1.7.1_en

Note: Compare the information in the Content Pack Details section with the *contentpack.properties* file. This file is located in the %USM_HOME%\filestore\contentpacks folder.

- The Content section lists the objects that are specified, according to the selected import criteria. The Objects are as follows:
 - Offerings (Services)
 - Service Option Groups
 - Forms
 - Events (rules, actions)
 - Report Data Objects
 - Report Variables
 - Resource Types
- 4. (Optional) If you have to create an inherited copy of any services through the Service Builder, select *one* of the following options:
Note: This selection cannot be reverted.
 - Click OK to copy all of the associated Service Option Groups.
 - Click Cancel to copy only Services and link to the original Service Option groups.

You have completed verifying ESX Content Pack import.

Verify Chargeback Services Import

Complete the following steps to verify if the chargeback services are installed successfully.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Requests, CA Automation Suite for Clouds, Server Automation Services.
3. Click VMWare ESX Management, Chargeback services.

4. Verify that the following chargeback services are listed:

- Service Offering Using VM Template
- Extend VM Reservation
- Return VM Reservation
- Service Offering Using Reservation Template
- Extend Template Reservation
- Return Template Reservation

You have completed verifying chargeback services import.

Add Cost Center and Department Details

You can configure the cost center and department name to enable Service Consumers to select these details while requesting a Virtual Machine.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, Content Configuration.
3. Click ASC Cost Center and Department.
4. Complete the following details:

Add Cost Center

Specifies a Cost Center name.

Type the name in the Enter Cost Center field, and click Add Cost Center. The cost center name appears in the Select Cost Center drop-down list.

Note: Optionally, to remove a cost center, select the cost center name from the drop-down list, and click Remove Cost Center. This step also removes the associated departments.

Add Department

Specifies a department name.

Select the Cost Center, type the name in the Enter Department field, and click Add Department. The new department name is associated with the selected cost center and appears in the Select Department drop-down list.

Note: Optionally, to remove a department, select the cost center under which the Department exists, select the Department, and click Remove Department.

5. Click Save.

You have configured the cost center and department details. The newly added cost center and department are listed in the service offering reservation forms.

(Optional) Hide the cost details in CA Service Catalog

Follow these steps:

1. Log in to the CA Service Catalog server.
2. Navigation to folder %usm_home%\explorer/service and open Serviceoptionpreview.xsl file

Example: C:\Program Files\CA\Service Catalog\view\webapps\usm\explorer\service

3. Edit the Serviceoptionpreview.xsl file.
4. Comment out the lines between the comments <!-- FOR EACH COST RATE ITEM --> and <!-- END FOR EACH COST RATE ITEM --> as follows:

```
<!-- FOR EACH COST RATE ITEM -->
<!--
<xsl:if
test="count(usm_rate_definition[item_type/LITERAL='3'])>0
">
<div class="data" style="margin-bottom:3px;">
<xsl:for-each
select="usm_rate_definition[not(item_id/LITERAL='-1') and
(item_type/LITERAL='3') and (position()>1)]">
<xsl:apply-templates select="."
<xsl:with-param
name="showpopuplink" select="$showpopuplink" />
</xsl:apply-templates><br />
</xsl:for-each>
</xsl:if> -->
<!-- END FOR EACH COST RATE ITEM -->
```

5. Delete all the generated translets.

6. Navigate to translets folder.

Example: C:\Program Files\CA\Service Catalog\view\translets

7. Delete all the .class files in the folder.

8. Log in to the CA Service Catalog.
9. Click Catalog, Configuration, Options, Request Management Configuration.
10. Click the Edit icon against the Access Control: Show Amount Column property.
11. Use arrows to remove all the user roles from the Selected list.
12. Click Update Configuration.
13. Restart the Service Catalog services.

The CA Service Catalog cost information is not displayed in the reservation forms.

Configure CA Process Automation Datasets for ESX

Configure the CA Process Automation datasets to provide data to the CA Automation Suite for Clouds Base Configuration automated processes for ESX. For more information about datasets, see the CA Process Automation documentation.

Note: Configure *Error Handling Parameters* in ASC_GlobalDataset and then proceed configuring the datasets that are listed in this topic.

The Datasets capture information of CA Server Automation and Reservation Manager Host, port, userid, and password to connect to CA Server Automation. These details help in provisioning, changing, and snapshot features. In addition, datasets also capture CA Service Catalog, CA Process Automation host, and login credentials to initiate the web services. These details help the solution to get the information from CA Service Catalog and update the request states.

Follow these steps:

1. Log in to the CA Process Automation console.

2. Click the Library tab from the home page.
3. Click the CA ASC folder.
4. Click ASC_GlobalDataset and Check Out.

Note: Delete all the unwanted or unused dataset values to ensure proper connection.

5. Click Login Parameters CHANGE ME and complete the following details:

userID

Specifies the CA Service Catalog Administrator user name.

Value: spadmin

password

Specifies the CA Service Catalog Administrator password.

businessUnit

Specifies the CA Service Catalog business unit name (This value is case-sensitive).

SAM_User

Specifies the CA Server Automation Administrator user name.

SAM_Password

Specifies the CA Server Automation Administrator password.

SpecAM_Touchpoint

If the CA Process Automation Agent is installed on CA Server Automation, then enter the Touchpoint value. This information is used for the datastore and VMware ESX provisioning.

6. Click APP URLs CHANGE ME and complete the following details:

SLCM_URL

Specifies the CA Service Catalog URL.

ITPAM_URL

Specifies the CA Process Automation URL.

SAM_URL

Specifies the CA Server Automation URL.

7. Click Misc Parameters CHANGE ME and complete the following details:

Administrator_Email

Specifies the administrator email.

VC_ESX_HostName

Specifies the ESX host name. This information is used in VMware ESX provisioning.

VC_Datacenter_Name

Specifies the Datacenter name. This information is used in VMware ESX provisioning.

VC_Server_Name

Specifies the vCenter server name. This information is used in VMware ESX provisioning.

SpecAM_Home

Specifies the CA Server Automation bin folder path. This information is used in VMware ESX provisioning.

SpecAMTouchpoint

Specifies the SpecAM Touchpoint. If the CA Process Automation Agent is installed on the CA Server Automation server, then enter the Touchpoint value. This information is used for the datastore and VMware ESX provisioning.

ESX_HostUser

Specifies the ESX host user name. This information is used in VMware ESX provisioning.

Value: root

ESX_OperationRetry

Specifies the retry count, when the operation fails.

Default: 3

ESX_WaitAttempts

Specifies the number of attempts during the wait period.

Default: 5

ESX_WaitTime

Specifies the time interval between each attempt.

Default: 60

StorageAdminOrAdminGroup

Specifies the storage admin.

WindowsAdmin

Specifies the Windows VM template parameters.

Specify the AdminPassword value for the default template. This value is used when the template is not available in the valuemap. Continue creating index values for each Windows VM Template:

Expand the Windows Admin folder, add Indexed Value. A new parameter set is added.

Expand Parameters, and add the following values:

Template

Specifies the name of the Windows virtual machine template.

AdminUserName

Specifies the user name of the virtual machine that accesses the newly provisioned Windows VM using the template.

Default: administrator

AdminPassword

Specifies the administrator password.

IsPasswordProvided

Specifies whether password is provided or not.

Change the parameter value to True if the password is provided.

Default: False

LinuxAdmin

Specifies the Linux VM template parameters.

Specify the AdminPassword value for the default template. This value is used if the template is not available in the valuemap. Continue creating index values for each Linux VM Template:

Expand the LinuxAdmin folder, Add Indexed Value. A new parameter set is added.

Expand Parameters, and add the following values:

Template

Specifies the name of the Linux virtual machine template.

AdminUserName

Specifies the user name of the virtual machine that accesses the newly provisioned Linux VM using the template.

Default: root

AdminPassword

Specifies the administrator password.

SSHPort

Specifies the port where SSH service is listening on the newly provisioned Linux virtual machine with the template.

Default: 22

UseSudo

Specify true if you want to use the sudo user in the Linux environment. For information about configuring the sudo user, see the [Update the sudoers File](#) (see page 207) section.

IsPasswordProvided

Specifies whether password is provided or not.

Change the parameter value to True if password is provided.

Default: False

PAMHome

Specifies the CA Process Automation installation path.

Example: C:\Program Files (x86)\CA\PAM

StorageOwner

Specifies the name of storage server that is configured with CA Server Automation.

8. Click *AD Login Parameters* CHANGE ME and complete the following details:

Adding these parameters allows you to toad secondary users as local administrator to the provisioned machine.

domainName

name of domain

Example: ca

domainAdmin

Specifies the domain administrator name.

domainAdminPassword

Specifies the domain administrator password.

isDomainAdminPasswordProvided

Specifies whether domain administrator password is provided or not.

Change the parameter value to True if the password is provided.

Default: False

9. Click Pam Parameters CHANGE ME and complete the following details:

pamMachineAdmin

Specifies the CA Process Automation machine administrator user name.

Default: Administrator

pamMachineAdminPassword

Specifies the CA Process Automation machine administrator password.

10. Click Storage and enter the details of the following storage services.

Note: If Storage is configured, highlight the Storage Value Definition for the storage integration.

- storageSpecAMTouchpoint
- storageSpecAM_Host_Admin
- storageSpecAM_Host_Password
- storageTierBronzeLabel
- storageTierSilverLabel
- storageTierGoldLabel

Note: If the CA Process Automation Agent has been installed on CA Server Automation, then enter the Touchpoint in the SpecAM_Touchpoint field.

11. Click Save.
12. Click Check In.
13. Close ASC_GlobalDataset.

You have configured the CA Process Automation content for CA Automation Suite for Clouds Base Configuration for ESX.

Update the sudoers File

Updating the sudoers file lets you issue commands from CA Process Automation using sudo without prompting for the root credentials. If the UseSudo parameter is enabled in the ASC_GlobalDataset, you update the sudoers file before creating the VM template.

Follow these steps:

1. Edit the /etc/sudoers file using the visudoers command.
2. Add the following entry:

```
# simple entry for issuing commands if the client does not need
# granularity
ascuser ALL=NOPASSWD: ALL

# detailed entry for permitting only those commands used by ASC
# for disk extension

ascuser ALL = NOPASSWD: /sbin/fdisk, /usr/sbin/pvcreate,
/usr/sbin/vgdisplay, /usr/sbin/vgextend, /usr/sbin/lvdisplay,
/usr/sbin/lvextend
```

3. Save and close the sudoers file.

Managing Virtual Machines in VMware ESX

VMware and Reservation Manager Terminology

Become familiar with the following terminology, which is used with both VMware and Reservation Manager:

Custom Specification

Custom Specifications are the XML files that contain the operating system configuration settings for customizing the guest operating system when a new virtual machine is created and deployed. Custom Specification is a VMware specific technology.

datastore

A *datastore* is the physical location where virtual machine files are stored and is both platform and host-independent.

host

A *host* is a physical computer that uses VMware software to run virtual machines; it is sometimes referred to as ESX or ESXi.

System Preparation Tool (sysprep)

A System Preparation Tool (sysprep) is used to configure Microsoft Windows XP Vista 2003, and 2008 operating systems. The Custom Specification file contains the sysprep settings.

Virtual Center (vCenter)

Virtual Center (vCenter) is the VMware management interface (server and client) that provides centralized control of the VMware infrastructure.

Virtual Machine

A *virtual machine* is software that emulates a computer system configuration including the software that runs on the system.

Virtual Machine template (VM template)

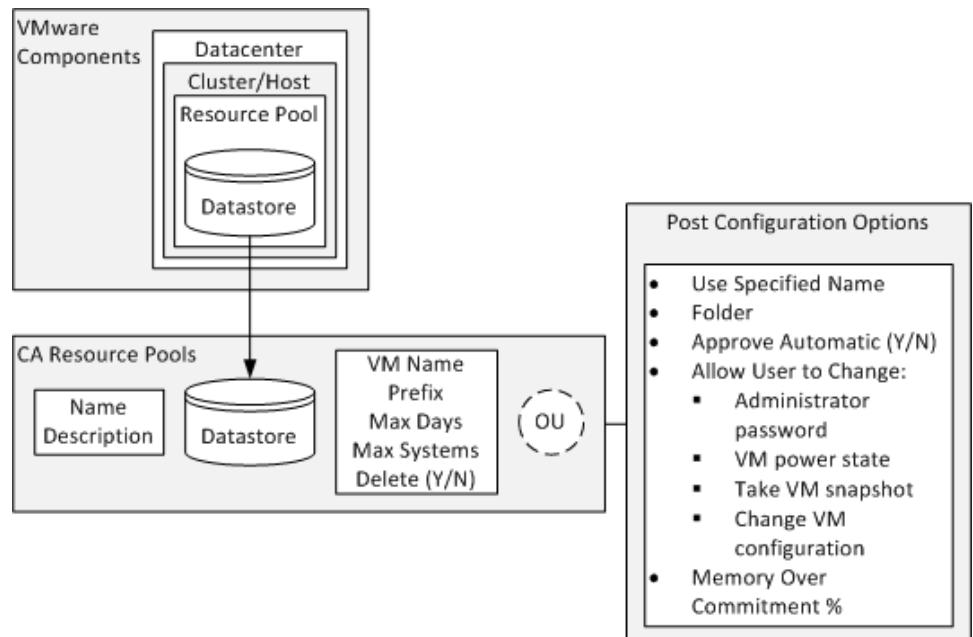
A *virtual machine template (VM template)* is an image of a virtual machine. You can use the image as a master copy to create and deploy new virtual machines.

Reservation Manager Components

Reservation Manager has four key components to configure: Resource Pools, System Images, Reservations Templates, and Organizational Units.

Resource Pools

When creating a Reservation Manager resource pool, you must name the resource pool and optionally provide a description. Select a datastore for the resource pool. The datastore list is populated from vCenter. Multiple datastores can be assigned to a resource pool. Resource pools have settings that can be configured by clicking the resource pool name, for example, naming conventions, and maximum reservation times. Additionally, to automatically approve reservation requests setting must be cleared. The Access policy can be defined by assigning an Organizational Unit (OU) to the resource pool. Organizational Units can be assigned later, if they are not yet configured.



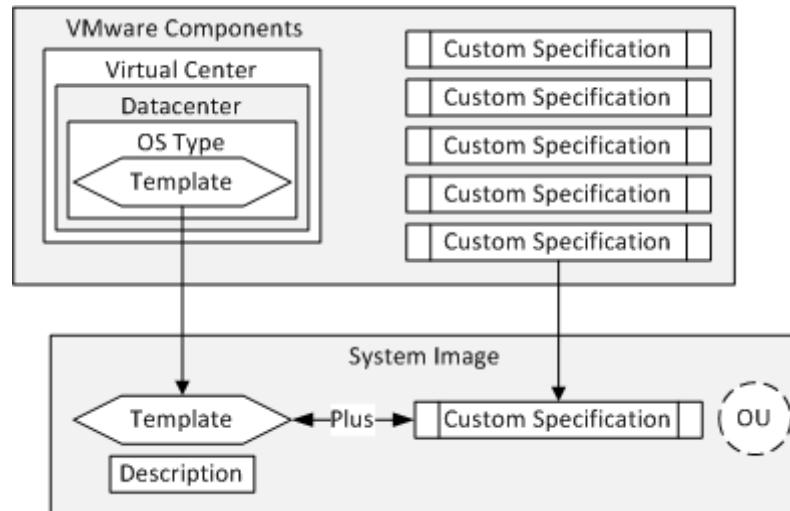
Note: When creating the organizational units, you can assign resource pools to the organizational units. Resource pools provide a detailed understanding about the functionality of organizational units.

After you create the resource pool, you can configure based on the advanced features that are listed in the previous graphic.

VMware and the Reservation Manager resource pools have similar purposes. In addition, the resource pools within the Reservation Manager allow you to define, configure, and limit how the resource pool is used.

System Images

In general, a Reservation Manager system image is the combination of a VMware template and a VMware custom specification file. The Reservation Manager system image lets you combine the VMware template and VMware custom specification file into a single entity. Use the image to create the virtual machines.



Reservation Manager lets you enhance, modify, and add to a basic virtual machine. You can configure the VMware template and VMware custom specification to build the smallest possible virtual machine of that type you plan to build. Commonly, you only require one VMware template per operating system type, and only one VMware custom specification file per operating system. The following table provides an example of an initial VMware template and VMware custom specification files and how they are combined into Reservation Manager system images:

VMware Template	CPU	RAM (GB)	HD (GB)
Windows XP	1	1	20
Windows 2003 Server Standard Edition	1	1	20
Windows 2003 Server Enterprise Edition	1	1	20
Windows 2008 Server Standard Edition	1	1	20
Windows 2008 Server Enterprise Edition	1	1	20
Red Hat Linux	1	1	20

VMware Custom Specification Files

Windows XP

Windows 2003 Server

Windows 2008 Server

Red Hat Linux

Reservation Manager System Images	VMware Templates	VMware Custom Specification Files
XP	Windows XP	Windows XP
W2K3Std	Windows 2003 Server Standard Edition	Windows 2003 Server
W2K3Ent	Windows 2003 Server Enterprise Edition	Windows 2003 Server
W2K8Std	Windows 2008 Server Standard Edition	Windows 2008 Server
W2k8Ent	Windows 2008 Server Enterprise Edition	Windows 2008 Server
RH	Red Hat Linux	Red Hat Linux

Note: You can use a VMware template only after creating a Reservation Manager system image. After the VMware template is defined as part of the Reservation Manager system image, the template is not available when you create a second system image. However, you can use system images multiple times when you create Reservation Manager templates.

You can assign organizational units to a system image and can add a description. Users can view the description when selecting a particular system image.

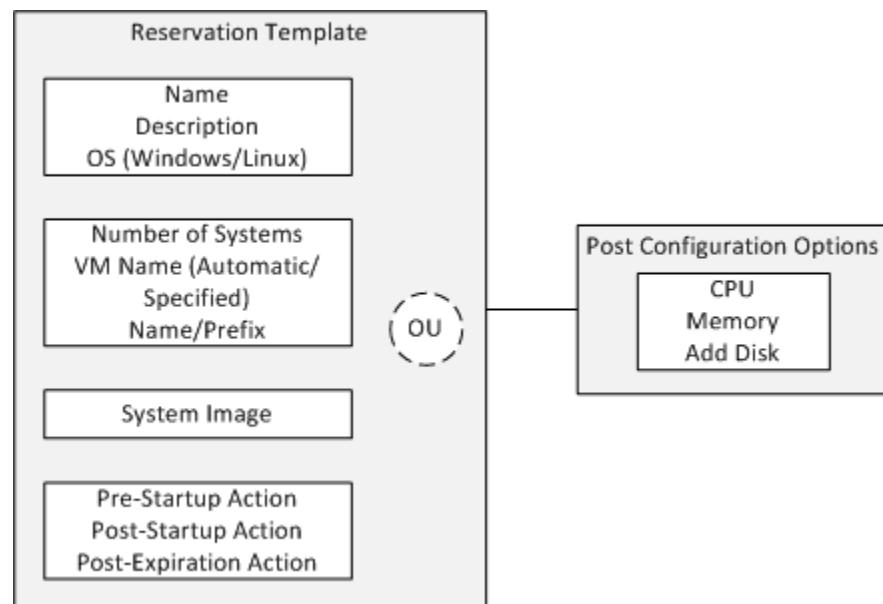
When a user uses Reservation Manager, they select a system image. They can later add more CPU, memory, or disk space. Similarly, use Reservation Manager Templates and select predefined virtual machines that are based on the basic system image that you defined.

Reservation Templates

The Reservation templates let you define nearly every aspect required when building a virtual machine, including machine settings and software installed.

Follow these steps:

1. Create the reservation template: defining basic information, assigning a system image, assigning a custom specification, allocation policy, any pre or post type actions, and access policy.
2. Edit the reservation template: defining CPU, memory, and additional hard disk space.



You can use system images multiple times in different reservation templates. Therefore, after you have a basic system image, you can assign it to multiple reservation templates. Using the previous example, every system created had 1 CPU, 1 GB of RAM, and a 20 GB of hard drive.

The following table shows an example of how you can expand the reservation template offerings using the basic system images that you created earlier:

Reservation Template	SSRM System Images	CPU	RAM (GB)	HD (GB)	HD (GB)
Windows XP Small	XP	1	1	20	
Windows XP Large	XP	1	1	20	20
W2K3 Standard - Bronze	W2k3Std	1	1	20	
W2K3 Standard - Silver	W2k3Std	1	2	20	20
W2K3 Standard - Gold	W2k3Std	2	2	20	40
W2K3 Standard - Platinum	W2k3Std	4	4	20	40
W2K3 Enterprise - Bronze	W2k3Std	1	1	20	
W2K3 Enterprise - Silver	W2k3Std	1	2	20	20
W2K3 Enterprise - Gold	W2k3Std	2	2	20	40
W2K3 Enterprise - Platinum	W2k3Std	4	4	20	40
W2K8 Standard - Bronze	W2k3Std	1	2	20	
W2K8 Standard - Silver	W2k3Std	1	2	20	20
W2K8 Standard - Gold	W2k3Std	2	4	20	40
W2K8 Standard - Platinum	W2k3Std	4	8	20	60
W2K8 Enterprise - Bronze	W2k3Ent	1	2	20	
W2K8 Enterprise - Silver	W2k3Ent	1	2	20	20
W2K8 Enterprise - Gold	W2k3Ent	2	4	20	40
W2K8 Enterprise - Platinum	W2k3Ent	4	8	20	60

Reservation Template	SSRM System Images	CPU	RAM (GB)	HD (GB)	HD (GB)
Red Hat - Development	RH	1	2	20	20
Red Hat - Marketing	RH	1	2	20	
Red Hat - Production	RH	2	4	20	40

Additionally, you can use the reservation template to define multiple virtual machines, so that by selecting a predefined reservation template, you can build two or three virtual machines. You can assign reservation templates to organizational units to limit their use.

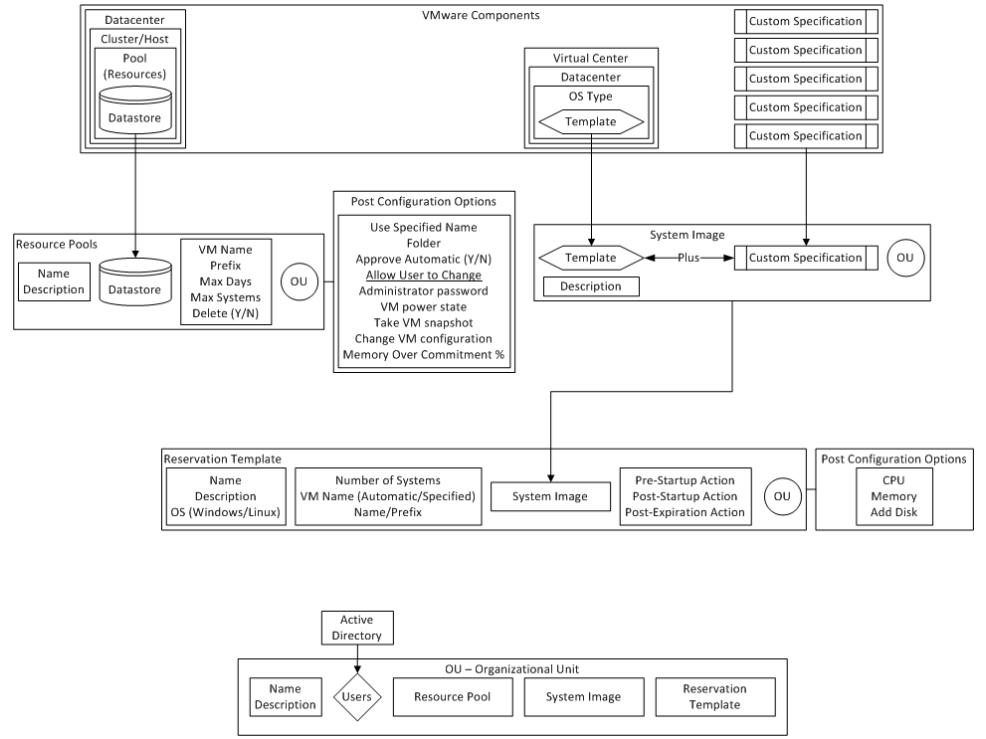
Organizational Units

By default, the Reservation Manager has a predefined organizational unit, named Public. You can use this organizational unit to allow everyone access to resource pools, system images, and reservation templates. However, you can create additional organizational units, which allows you to limit who can access the various components.

Reservation Manager is integrated with CA EEM. You can define users in CA EEM and then add the users to a particular Organizational Unit. CA EEM works with the Active Directory of your company. You can easily import user accounts and then add the users to organizational units as required. Similarly, you can remove users from organizational units.

VMware and Reservation Manager Diagram

The following graphic shows the relationships among the VMware and Reservation Manager components.



Prerequisites for Supporting Reservations of Virtual Machines

Before the Reservation Manager deploys virtual machines for usage, identify one or more VMware ESX servers or clusters for use. Then, define which resource pools on each VMware ESX server or cluster are targets for the virtual machine creation. To determine whether a VMware ESX server can create a virtual machine, the Reservation Manager must calculate the amount of memory available for the new virtual machines. The calculation is made on the VMware ESX servers.

If the resource pools on the VMware ESX server have defined memory limits, the Reservation Manager requires exclusive access to the resource pool. The resource pool is targeted to determine the resource availability for the future.

In the absence of memory limits at a resource pool level, the Reservation Manager calculates the amount of memory available to virtual machines. The calculation is made at the VMware ESX server level. The Reservation Manager requires exclusive use of the VMware ESX Servers to determine the accurate resource availability in the future.

Note: Resource pools and virtual machine templates are added to the vSphere Datacenter and the folder in which they are defined. You cannot use the resource pools and templates that were previously added to the Reservation Manager in the following instances:

- The VMware datacenter is renamed
- The virtual machine templates are moved to a different folder

Ensure to stabilize the vSphere structure before adding these items.

Setting up VMware Environment

Before you begin configuring the Reservation Manager, ensure to set up the VMware environment and make it operational.

Ensure the following details in the VMware infrastructure:

1. Test that you can access vCenter by its URL (Default is https using port 443).
2. VMware ESX host servers are connected and have at least one virtual machine or template registered.
3. Datastores are connected and viewable within vCenter.

Note: By default, the datastores are generated with a nonintuitive naming convention. If you want to change the name, ensure to change it before configuring with Reservation Manager.

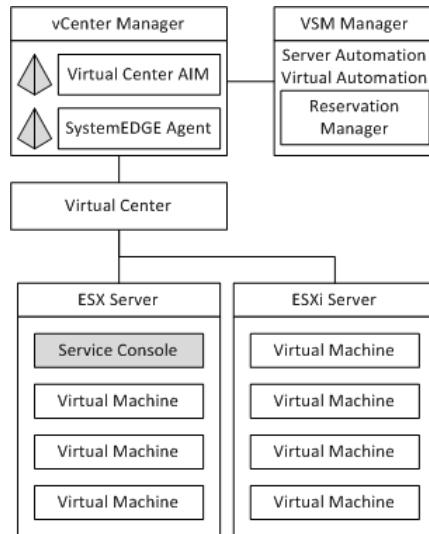
4. Create a virtual machine template for each operating system that you want to deploy.
5. Verify that sysprep is installed if Windows XP and 2003 Standard and Enterprise Servers are deployed.
6. Create a Custom Specification file for each operating system.

Note: Because the Reservation Manager can customize these Custom Specification files, create them as generic as possible. For example, the Computer Host Name (NetBIOS Name) set to “Use the virtual machine name” and the Network have DHCP enabled.

How to Connect Reservation Manager to VMware vCenter

All communication from the Reservation Manager to the VMware infrastructure happens through the vCenter. The connection between the Reservation Manager and the vCenter is established during the installation. However, as the VMware environments often change or new vCenter servers are brought online, ensure that you connect Reservation Manager to the vCenter.

The following procedure provides the basics for making this connection.



You actually perform two connections:

1. Connect to VSM Manager
2. [Connect to vCenter AIM](#) (see page 220) —a small agent-type component.

Typically you install vCenter AIM in the same machine where you have the VSM Manager, however it is not mandatory as you require two connections.

The vCenter AIM is comprised of two components:

- SystemEDGE Agent—an SNMP-based agent
- vCenter AIM—a plug-in to the SystemEDGE Agent that enables the communication between Reservation Manager and vCenter.

Connect to the VSM Manager

Important! Before connecting to the VSM Manager, verify the fully qualified domain name of the vCenter server using the *ping* and *nslookup* utilities.

Follow these steps:

1. Log in to the CA Server Automation.
2. Click Management, Administration.
3. Click vCenter Server under Provisioning.
4. In the top half of the window, click Add (+) in the upper right-hand corner to add the vCenter.
5. Complete the vCenter details and click OK:

A green check mark appears under Status indicating that the credentials are validated.

6. Click OK to Add the Virtual Center Server.

You have connected to the VSM Manager.

Connect to vCenter AIM Server

You next connect to the vCenter AIM Server, which is where the vCenter AIM is installed (most commonly on the VSM Manager). To make this connection, open a command prompt and navigate to the location of a utility program named NODECFGUTIL. Depending on your installation location, you can typically find this utility in the \Program Files\CA\(\VSM Manager)\SystemEDGE\plugins\AIPCommon folder.

Follow these steps:

1. Open a command prompt and enter *nodecfgutil*.
2. Type 1 to Install Managed Node and press Enter.
3. Type the number next to VMware vCenter (3) and press Enter.

4. Enter the credentials similar to the Virtual Center server that you entered the VSM Manager connection:
 - Fully Qualified Server Name. For example, forwardinc-vc.forwardinc.com.
 - User Name and Password: Enter the user name and password where the user has sufficient rights to perform all tasks in vCenter.
 - Port: Enter the port number or accept the default 443 value.
 - Protocol: Enter the protocol or accept the default https value.
5. Press Enter.

The utility indicates that you successfully installed the vCenter.

6. Press any key to continue.
7. Type 0 to exit the nodecfgutil utility.
8. Log in to the CA Server Automation.
9. Click Management, Administration.
10. Click vCenter Server under Provisioning.
11. Verify that the correct information for the vCenter AIM Server and vCenter Server are in the lower half of the screen.

Both VSM Managers use this connection to discover, manage, and monitor the virtual infrastructure. After this connection is made, depending upon the size of the existing VMware environment, the VSM Manager performs numerous tasks discovering and configuring the VMware environment.

Access Reservation Manager

Access Reservation Manager as the administrator of the VSM Manager.

Log in to the Reservation Manager using the CA Server Automation administrator user credentials and the following URL:

<https://servername:port/ssrm>

The Tasks screen opens and provides the functionality available to you as an administrator and based on the products in your enterprise.

You configure the following details in the Reservation Manager:

1. Manage your organizational units
2. Manage your resource pools
3. Manage your system image inventory
4. Manage your reservation templates

Create Organizational Units in Reservation Manager

The organizational units define the system images available to users within the organizational unit.

Follow these steps:

1. Create a group or import existing groups for each organizational unit in Active Directory.
2. Assign the users in Windows Active Directory to each user groups.
3. Log in to the Reservation Manager using the CA Server Automation administrator user credentials and the following URL:
`https://servername:port/ssrm`
See your [Installation Worksheet](#) (see page 19) for these values.
4. Click Administer Your Reservation Manager.
The Administration page opens.
5. Click Manage your organizational units
The organization unit page opens.
6. Select Add from the Actions drop-down list.
The Add Organizational Unit wizard opens on the Define Organizational Unit page.
7. Enter an organizational unit name, description, and click Next.
The Select Users/Attributes page opens.

8. Select the Identity Type, Attribute, Operator, and Value to display the users or user groups to assign to the organizational unit.

9. Use the arrows to move one or more users or user groups from the Available Users/Attributes window to the Selected Users/Attributes window.

10. Click Next.

The Specify Pool Access page opens.

11. Select the resource pools for the organizational unit.

12. Click Next.

The Specify Image Access page opens.

13. Select the system images for the organizational unit.

Click Next.

The Specify Software page opens.

14. Select the software groups for the organizational unit.

Note: The software packages only appear if they have been added.

15. Click Next.

The Manage Reservation Template Access page opens.

16. Select the reservation templates for the organizational unit.

17. Click Finish.

The Organizational Units page opens.

18. Verify that the organizational unit appears correctly.

Note: Double-click an organizational unit to edit the properties.

You have added an organizational unit.

Create and Configure Reservation Manager Resource Pools

To build the Reservation Manager resource pools, you first create the resource pool and edit it for the advanced settings and features.

Note: The addition of resource pools is performed in context to the vSphere Datacenter at the time they are added. If the VMware datacenter is renamed, the resource pools that are defined in the Reservation Manager are no longer usable. Therefore, it is important to stabilize the vSphere structure before adding resource pools.

Follow these steps:

1. Log in to the Reservation Manager using the CA Server Automation administrator user credentials and the following URL:
`https://servername:port/ssrm`
See your [Installation Worksheet](#) (see page 19) for the values.
2. Click Administer Your Reservation Manager.
The Administration page opens.
3. Click Manage your resource pools.
The Resource Pools page opens.
4. Select Add Virtual Pool from the Actions drop-down list in the upper right corner of the Resource Pools list.
The Add Virtual Pool wizard opens to the Specify Pool page.
5. Enter the pool name and an optional description for the Reservation Manager resource pool, and click Next.
This associates with one or more Reservation Manager resource pools.
Note: Resource pool names are read-only after the pools are saved.
The Specify Virtual Resource Pools page opens where you specify the virtual resource pools that get assigned.
6. Verify or select the vCenter server where the datastore gets assigned to the Reservation Manager resource pool.
7. Select Add from the Actions drop-down list.
The Add Resource Pool dialog opens so that you can assign VMware virtual resource pools to this Reservation Manager resource pool.

8. Select a data center name, a cluster, or ESX server resource pool as the target for VM creation, and one or more datastores.
9. (Optional) If your site is configured to use storage tiers, select an existing tier or enter new a tier. Select this option for each datastore to assign to the Reservation Manager resource pool.
10. Click OK.

The pool name *Resources* is a special case pool name that you select to indicate that all resources on the cluster or ESX server are available for use.

Note: You can view the usage for individual data stores before making your selection. The data stores must always have enough space to store all the virtual machines that are targeted to this virtual resource pool.

You are returned to the previous page and a new row is added to the table. You can add as many cluster or ESX server resource pools to this Reservation Manager resource pool as you want.

The only limitation is that the same VMware vCenter server manages the resource pools. The selected cluster or ESX server resource pools are not associated with a different Reservation Manager resource pool.

11. Click Next.

The Configure Settings page opens.

12. Complete the following fields. These fields specify the limits on the duration and number of virtual machines a user can request when submitting a reservation for resources.

VM Name Prefix

Specifies a prefix for all virtual machine names that are built in the Reservation Manager resource pool. You can also use several variables instead of a specific name: %DATACENTER%, %ORGUNIT%, %PROJECTID%, %RESERVATIONID%, %RESOURCEPOOL%, %USERNAME%, or %HOSTSYSTEM%.

VM Base Name

Specifies the VM base name

VM Name Index Format

Specifies VM name index format

VM Name Suffix

Specifies the VM name suffix

Maximum Days

Limits the reservation length to a specified number of days.

Maximum Systems per User

Limits how many systems a user can reserve from the pool.

ITCM Domain Manager

Specifies the CA IT Client Manager domain manager that manages the software that is installed on the virtual machines. Verify or enter the value.

Scalability Server

Specifies the scalability server that installs the software to the virtual machines on the Reservation Manager resource pool. Verify or enter a value.

Delete After Power Down

Specifies the post processing that is performed at the reservation end for the virtual machines that are associated with this pool. This option is selected by default, so machines are powered down and destroyed at the reservation end. If unselected, the virtual machines are powered down only.

Grace Period

Specifies the grace period.

13. Click Next.

The Specify Access Policy page opens.

14. (Optional) Select the organizational units whose members are granted access to the systems in the selected virtual resource pool, then click Finish.

You can click Finish to skip the step in the following cases:

- When an organizational unit that is granted access to the resource pool is not listed.
- When you are not sure of organizational units to grant access.

You can grant access to the resource pool later.

The Reservation Manager creates a resource pool with the same name as the vCenter resource pool and displays a confirmation message when the process completes successfully. The wizard closes and the Add Virtual Pool page displays the new virtual resource pool in the Resource Pools list.

The Resource Pool page opens.

15. Verify that the Reservation Manager resource pool was created.

16. Double-click a resource pool.

The Resource Pools Details page opens. This page contains three tabs: Properties, Resource Pool Details, and Access Policy.

17. Click the Properties tab and provide the information.

See the CA Service Catalog section on your [Installation Worksheet](#) (see page 19).

18. Clear “Automatically approve reservation requests” checkbox.
19. Select “Allow user to specify the Administrator password” checkbox.
20. Select “Allow users to take a VM snapshot” checkbox. Also, update the Maximum Number of Snapshots count as required.
21. Click the Resource Pool Details tab.
The Resource Pool Details page opens.
22. (Optional) Edit or assign more datastores.
23. Click the Access Policy tab.
The Access Policy page opens.
24. (Optional) Add, edit, or remove any organizational units.
25. Click OK.

You have created and configured a resource pool.

Create and Configure Reservation Manager System Images

You now create the system images for the virtual machines.

Follow these steps:

1. Log in to the Reservation Manager using the CA Server Automation administrator user credentials and the following URL:
`https://servername:port/ssrm`
See your [Installation Worksheet](#) (see page 19) for these values.
2. Click Administer your Reservation Manager.
The Administration page opens.
3. Click Manage your system image inventory.
The System Images page opens. This page lists the inventory of operating system images and virtual machine templates that are available for users to select when reserving systems. From this page, you can define the operating system images or virtual machine templates to make available to users.

4. Select Add VM Template from the Actions drop-down list to add new virtual machine templates to the inventory.

The Add VM Template wizard opens on the Select Image page.

The information automatically populates based on the first available template in vCenter.

Note: After you assign a VMware template to a Reservation Manager system image, you cannot assign it to another system and the template does not appear again.

5. Specify the following vCenter resources first to add the template to the inventory: vCenter Server, Data Center Name, and Guest OS Type. Then select the virtual machine template from the Template Name list, add a template description, and click Next.

Note: Templates for VMware reservations must be in the same data center as the resource pools available to users.

The Specify Custom Specification page opens.

6. Select the custom specification file to use to tailor settings for the virtual machines to deploy using this template, and click Next.

Note: Because of the guest operating system type (Windows or Linux) you selected, only the VMware custom specification files for that operating system type appear. You can assign a VMware custom specification file to multiple Reservation Manager system images.

The Specify Software page opens.

Note: This screen is available only if you have the CA Server Automation installed and integrated with the CA IT Client Manager (Software Delivery). After you have imported the Software Delivery packages and made them available, they appear in the Available Software Group window.

7. Move all software that you want to install on the system image from the Available Software Group to the Selected Software Group.

The Available Software Group list contains software that the administrator has identified as being compatible with the selected operating system. This list is filtered to display only software that you are authorized to access. Authorization is based on the organizational unit that your user name has been assigned to.

The selected software is installed on the system in the order it is listed in the Selected Software Group list. Use the up and down arrow buttons to modify the order of software in the list.

8. Click Next when finished. You do not have to select any software on this page.

The Specify Access Policy page opens.

9. Select the organizational units whose members are granted access to this virtual machine template, then click Finish.

Note: Before you grant access to users, grant the rmadministrators user group access so you can test creating reservations for virtual machine templates.

10. Click Finish to skip the step in the following cases:

- When an organizational unit that is granted access to the template is not listed.
- When you are not sure of organizational units to grant access.

You can grant access to the resource pool later.

The System Images page opens and lists the template that has been successfully added to the inventory.

11. You can double-click a system image to edit it.

You have created and configured Reservation Manager system image.

Policy Management

For information about creating and managing policies, see the *Managing Policies* chapter in *CA Server Automation Administration Guide*.

Specify a Prefix for Virtual Machine Names

You can specify a prefix for VMware virtual machines at the resource pool level. A prefix provides a consistent naming convention.

Follow these steps:

1. Log in to the Reservation Manager using the CA Server Automation administrator user credentials.
2. Click Administer Your Reservation Manager.
The Administration page opens.
3. Click Manage your resource pools.
The Resource Pools page opens, and lists existing pools.
4. Double-click a resource pool.
The Resource Pool details page opens, with the Properties tab displayed.
5. Select the values for the following fields:

VM Name Generation

Lets you choose whether to use a prefix or a specified name. Reservation Manager appends the reservation ID to the name or prefix.

Automatic using prefix

Lets you enter a prefix for the VM name.

Use specified name

Lets you specify a name in the VM Name field.

Default: Automatic using prefix

VM Name Prefix

Specifies a VM name or prefix for the virtual machine names.

Default: none

Limits: Ten alphanumeric characters when the *Automatic using prefix* field is selected. 15 alphanumeric characters when the *Use specified name* field is selected.

Note: When creating the virtual machine names using either a prefix or a specified name, the name must contain alphanumeric characters or a hyphen. If you use any other characters, they are automatically replaced with a hyphen.

VM Name Index Format

Specifies the VM name index format

Default: Automatic

6. Click OK.

You have specified the prefix.

Provision VMware ESX Host

A host is a physical machine on which the ESX software is installed. Before Service Consumers begins reserving virtual machines, as a Service Provider, you provision the ESX host for the virtual machines for each organizational unit. As your organization grows, you can add more ESX hosts.

Follow these steps:

1. Log in to CA Service Catalog.

Note: Your enterprise administrator can provide you with the necessary URL and access credentials.

2. Click Requests, CA Automation Suite for Clouds, Server Automation Services, Infrastructure Management.

The Infrastructure Management offerings page open.

3. Click Provision ESX Host.

The Provision ESX Host page opens.

Note: Fields marked with a red dot are required.

4. Select an Organizational Unit from the drop-down list, which is the organizational unit that the ESX host machine is provisioned for.

The System Image drop-down list populates. This list of available ESX images are loaded from CA IT Client Manager.

5. Select a System Image from the drop-down list.

The System Image Details panel populates with the system image Description and Operating System and the Software field populates with the available software.

6. Complete the following fields:

Date and Time

Specifies the start and end date and time at which the ESX host is available.

Quantity

Specifies the number of systems available in the ESX host.

CPUs

Specifies the number of CPUs available in the ESX host.

Memory (GB)

Specifies the minimum amount of memory in GB available in the ESX host.

Disk Space (GB)

Specifies the minimum disk space available in GB available in the ESX host.

7. Enter an Administrator Password to access the ESX host and then enter the password again to confirm.

8. Click Fetch Available Systems.

The Available Systems field populates with the systems available in Reservation Manager.

9. Ctrl+Click the system that you want to use in the Available Systems field.

Note: The Notification Email Address shows the email identification of the requester. You cannot edit this field.

10. Click Add to Cart to continue adding more requests to the cart.

The request is added to the cart.

11. Click Check Out when you complete adding the requests.

12. Review your request details, and click Save and Submit.

A confirmation displays indicating your request was submitted.

Integrate CA Business Intelligence with CA Service Catalog

Prerequisites for CA Business Intelligence Integration with CA Service Catalog

Verify the following items before you start the CA Business Intelligence configuration:

- Ensure CA Service Catalog is installed.
- Ensure CA Business Intelligence infrastructure has been installed and validated.
- Ensure Java JDK Version 1.7 or above (64 bit) is installed.
- Use the 32-bit ODBC Administrator to [Create an ODBC to MDB of the CA Service Catalog database](#) (see page 235) on the CA Business Intelligence Server. See the Installation Worksheet under CA Business Intelligence, CA BI Data Source Name to MDB.

Note: Use the usmuser login for the System DSN ODBC connection.

Create DSN and ODBC Connection for CA Service Catalog

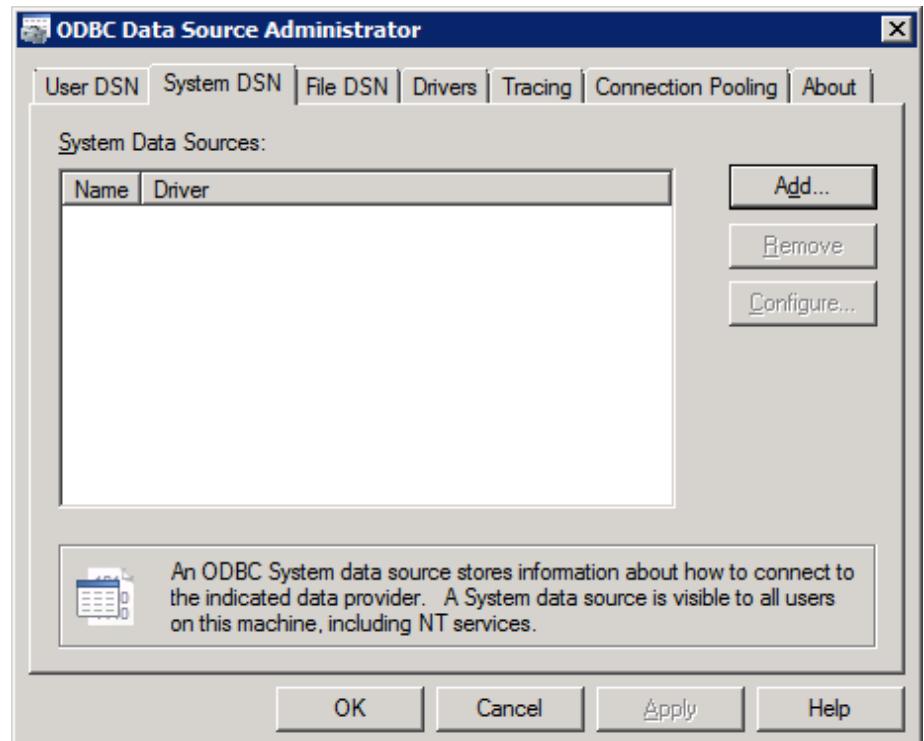
You can create an ODBC connection to the CA Service Catalog Database.

Follow these steps:

1. Run the *odbcad32.exe* file from the following location:

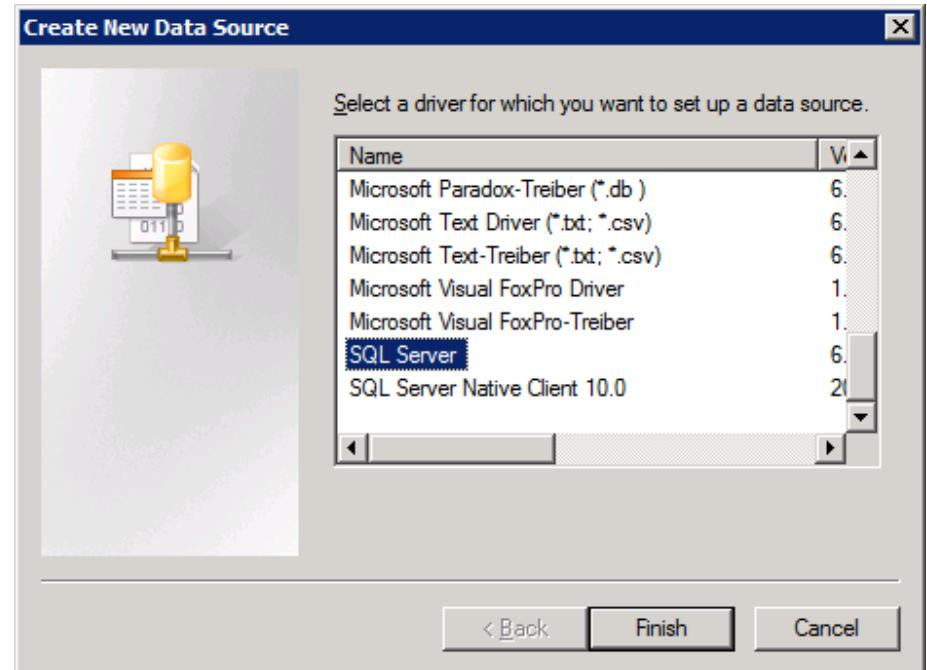
c:\Windows\SysWOW64\

The ODBC Data Source Administrator dialog opens.



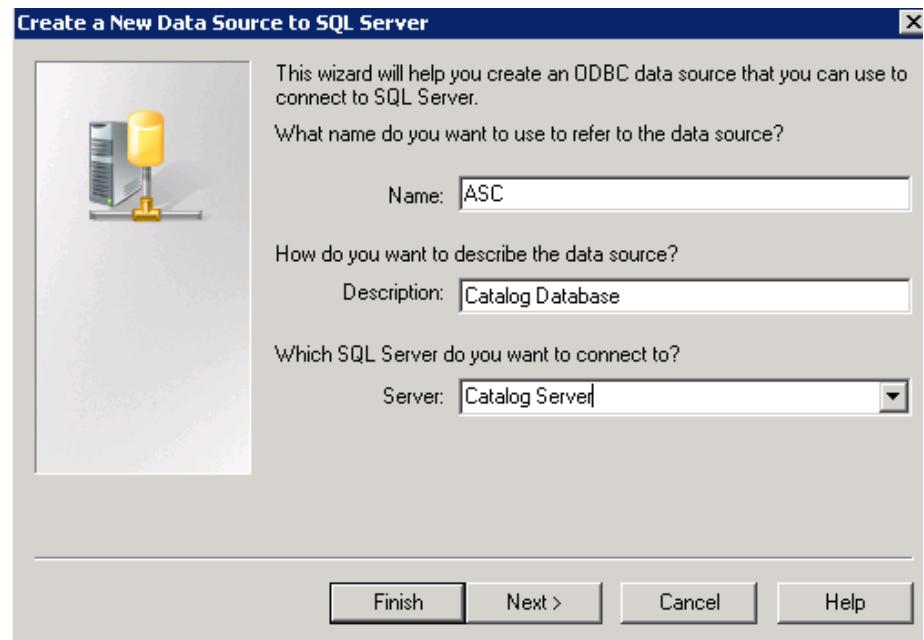
2. Click the System DSN tab, and click Add.

The Create New Data Source wizard opens.



3. Select SQL Server from the driver list and click Finish.

The *Create a New Data Source to SQL Server* page opens.



4. Enter the following parameters.

Name

Specifies the name of the database.

Example: ASC

Description

(Optional) Specifies the description of the data source.

Example: Catalog database

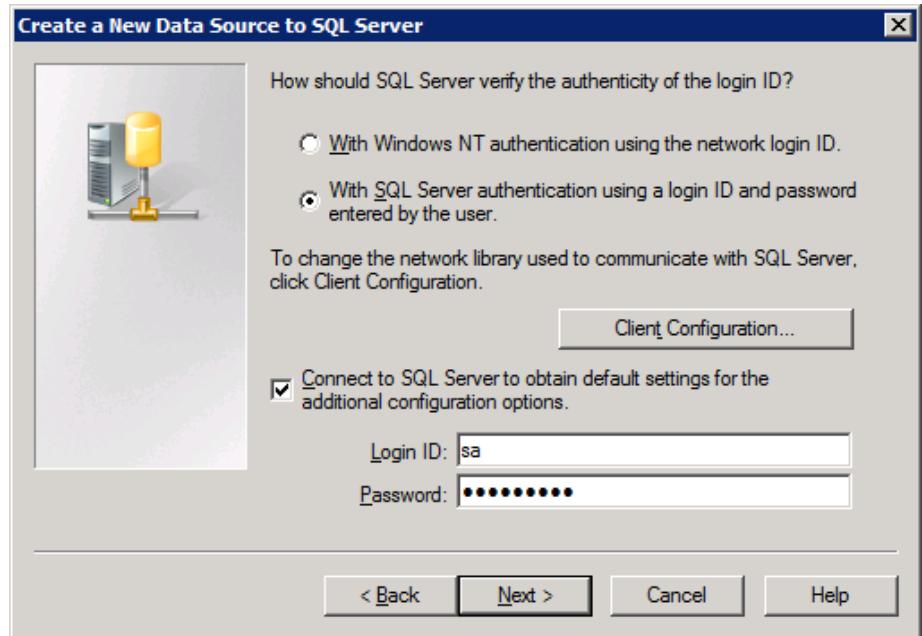
Server

Use the drop-down list and select the server where the database resides. If a Named Instance of SQL is used, then enter <SQL Server>\<Named Instance>.

Default: Catalog Server

5. Click Next:

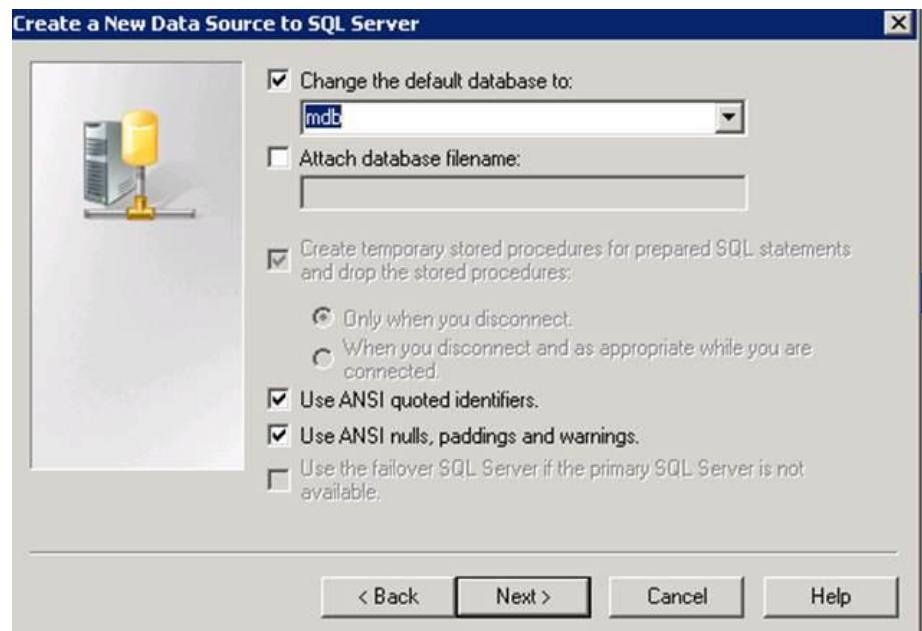
The Create a New Data Source to SQL Server page opens.



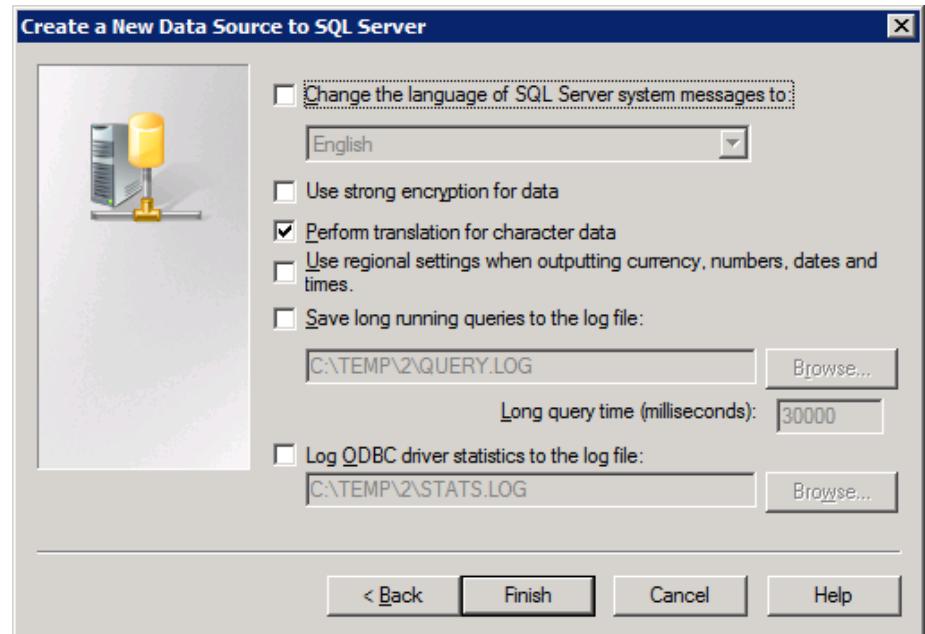
6. Select the With SQL Server authentication using a login ID and password from the user option.
7. Select the Connect to SQL Server and obtain default settings for the additional configuration options.

8. Type a Login ID and Password with access to the MDB database, and click Next.

The Microsoft SQL Server DSN Configuration page opens.

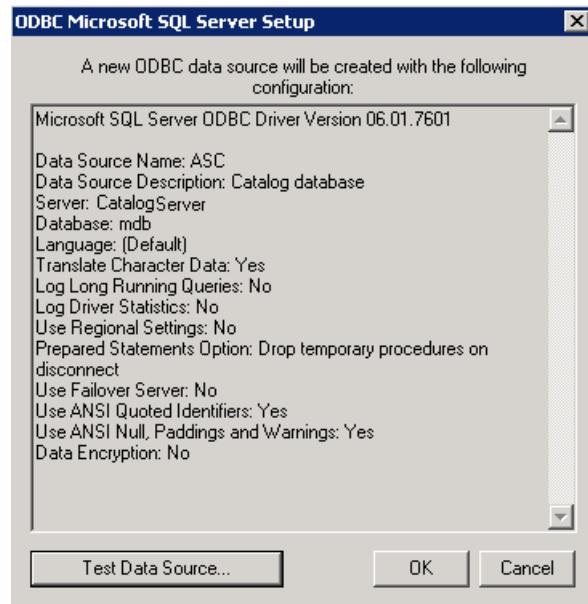


9. Select the Change the default database to check box and select the database name (mdb) from the drop-down list.
10. Click Next.



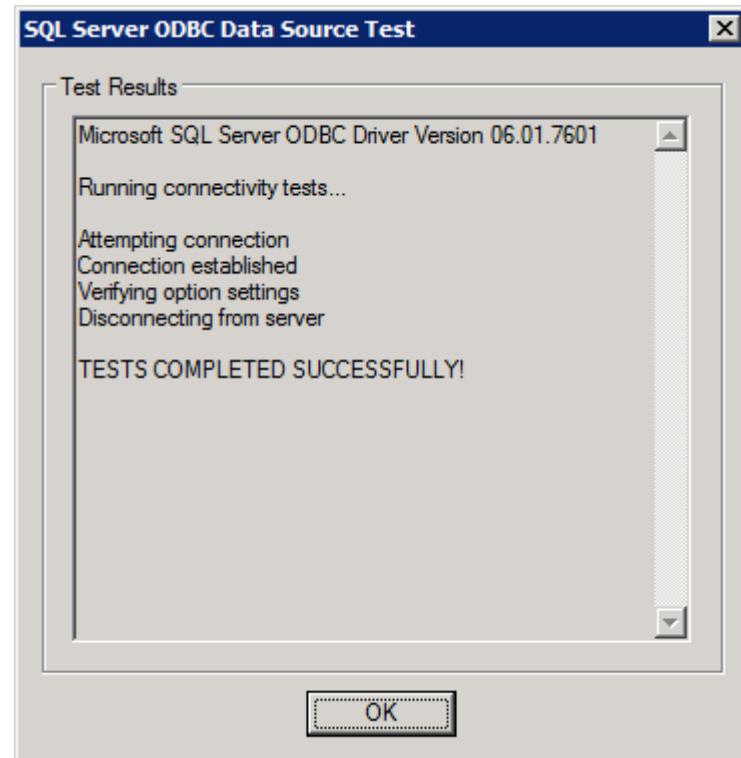
11. Click Finish.

The ODBC Microsoft SQL Server Setup page opens.



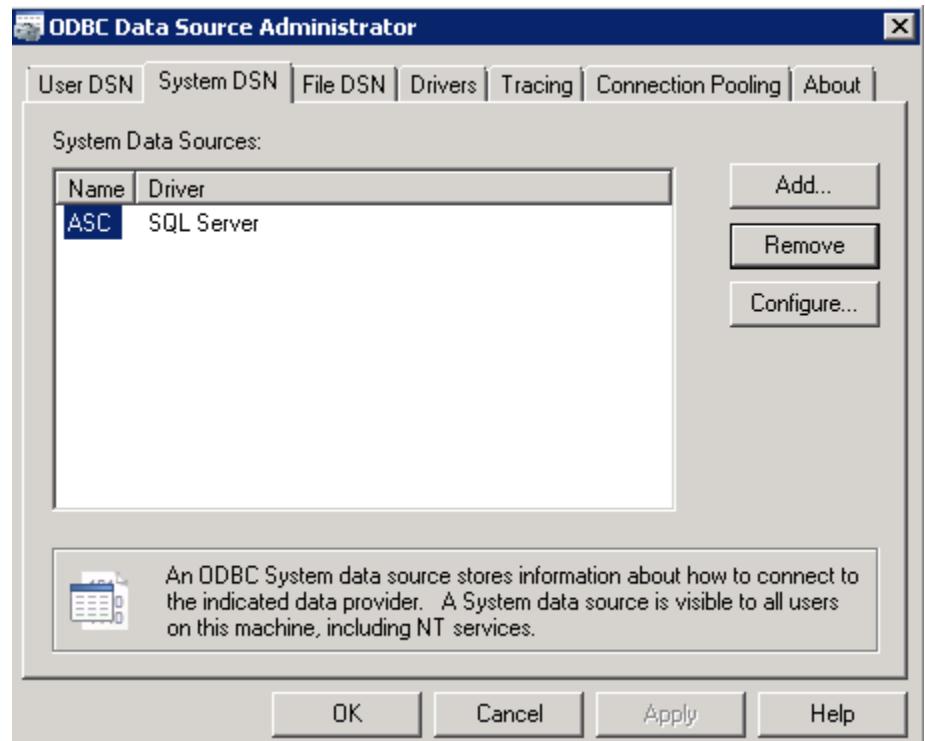
12. Click Test Data Source and verify the connection.

A confirmation message appears.



13. Click OK to close the message and click OK to close the ODBC Microsoft SQL Server Setup page.

The ODBC Data Source Administrator page opens.



Note: Record the ODBC name of CA Service Catalog in the [Installation Worksheet](#) (see page 19) under CA Business Intelligence.

14. Click OK.

Note: If the MDB Database used by CA Service Catalog and Software Delivery are created, a second ODBC Connection will need to be created to this MDB Database. This step is performed in the Post-Configuration section, but you could perform now if products are installed and the MDB Database is created.

The DSN and ODBC connection are complete.

Import CA Service Catalog Reports

Perform the following steps to import Business Intelligence Archive Resource (BIAR) file.

Follow these steps:

1. Set Java home on the CA BI Reporting server.
 - a. Right-click My Computer on your desktop and select properties.
 - b. Click the Advanced Tab.
 - c. Click the Environment Variables.
 - d. Under System Variable, click New.
 - e. Enter the variable name as JAVA_HOME.
 - f. Enter the variable value as the install path for the Development Kit.
Example: C:\Java\JDK
 - g. Click OK.
 - h. Click Apply Changes.
2. Copy the BIAR folder from the CA Business Intelligence media\Disk1\cabi\biconfig directory to the CABI Machine in any directory(for example, C Drive(C:\biconfig)).
Note: If the biconfig folder does not exist under the C drive, then create the biconfig folder.
3. Copy the SLCM_universe.biar file from \\<SLCM Application Server>\C\$\Program Files\CA\Service Catalog\reporting\CABI\biar to the C:\biconfig folder.
4. Copy xml_biar_import.xml file from the biconfig\Samples folder into the biconfig root folder and rename to xml_biar_import.catalog.xml.

5. Edit `xml_biar_import.catalog.xml` file so that it reads similar to the following example, which is outlined more generally in Step 4:

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <!-- Import BIAR file -->
  <step priority="1">
    <add>
      <biar-file name="C:\biconfig\SLCM_universe.biar">
        <networklayer>ODBC</networklayer>
        <rdms>MS SQL Server 2008</rdms>
        <username>sa</username>
        <password>password</password>
        <datasource>ASC</datasource>
        <server>Catalog Server Name</server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

Note: Verify that the name for `<datasource>` matches the DSN name specified in the [Installation Worksheet](#) (see page 19) under CA Business Intelligence, CA BI Data Source Name to MDB. For example, in the screenshot above, the DSN name is ASC.

6. In the Command Prompt window, change the directory to the `C:\biconfig` location, and then execute `biconfig.bat` to import the BIAR file using the following command:

```
biconfig -h "<CABI_Server_Name>" -u "<administrator>" -p
"<admin_password>" -s "secEnterprise" -f
"xml_biar_import.catalog.xml"
```

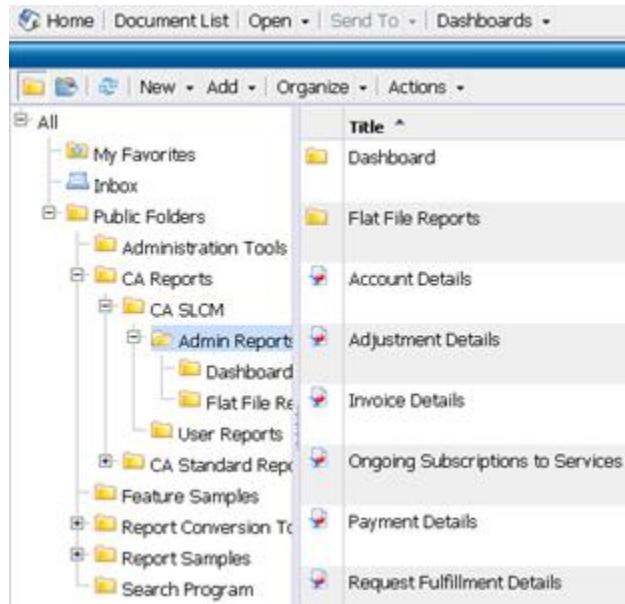
7. Verify the import, as follows:

- a. Review the biconfig.log file in the biconfig folder:

This file lists the status of the import. This file also includes error messages if the BIAR file is not imported successfully.

- b. Log in to InfoView as a BusinessObjects Enterprise administrator.

- c. In InfoView, verify that you can view the CA SLCM Reports under Public Folders/CA Reports/CA SLCM.



8. Change the catalog administrator password (default: spadmin).

Note: The new password must match the password that spadmin uses to log in to CA Service Catalog.

To set the password, perform the following steps:

- a. Log in to the BusinessObjects Enterprise Central Management Console.
- b. Click Users and Groups link under the Organize column.
- c. Click User List.

- d. Double-click spadmin to open the Properties page.
- e. Specify the password in both the Password and Confirm fields.
- f. Click Save & Close. Log out from the Central Management Console when done.

Importing of the CA Service Catalog reports is complete. See *CA Service Catalog Integration Guide* for complete steps on importing CA Service Catalog reports.

Configure CA Business Intelligence in CA Service Catalog

Follow these steps:

1. Log in to CA Service Catalog as an administrator (for example, spadmin).
2. Click the Administration, Configuration, CA Business Intelligence.

Options	CA Business Intelligence(CABI)		Launch
	Property	Value	Modify
CA APM Web Services	CMS Host Name	ASC-BOXE	
CA Automation Suites Reservation Manager	CMS Port Number (1-65535)	8080	
CA Business Intelligence(CABI)	Enable HTTPS	No	
CA Business Service Insight	Host Name	ASC-BOXE	
CA CMDB	Port Number (1-65535)	8080	
CA CMDB Visualizer			
CA Process Automation			
CA Service Desk			
CA Workflow			
Event Manager			
File Store Information			
Mail Server			
Portal			
Request SLA			
Rule Engine			
Server Information			
Single Sign On Authentication			
System Information			
User Default			

3. Modify the following property values, as appropriate:

CMS Host Name

Enter the host name of the Business Objects XI CMS is installed.

CMS Port Number

8080

Enable HTTPS

No

Host Name

Enter the host name where the Business Objects XI InfoView is installed.

Port Number

8080

4. Click Launch in the upper right corner and validate that you can log in to BOXI InfoView.
5. Close Business Objects XI InfoView.

CA Service Catalog is integrated with CA Business Intelligence.

Note: The password of the CA Service Catalog user must match the password of the CA Business Intelligence user.

Configure Trusted Authentication

See the *CA Service Catalog Integration Guide* for more information about configuring the trusted authentication between CA Service Catalog and CA Business Intelligence.

Follow these steps:

1. Log in to Central Management Console as an administrator.
2. Click Authentication in the Manage section.
3. Double-click Enterprise, and perform the following steps on the Enterprise screen:
 - a. Select the Trusted Authentication is Enabled check box.
 - b. Type a string of characters (like a password) in the Shared Secret field.
 - c. Click Update to save the changes and close the window.

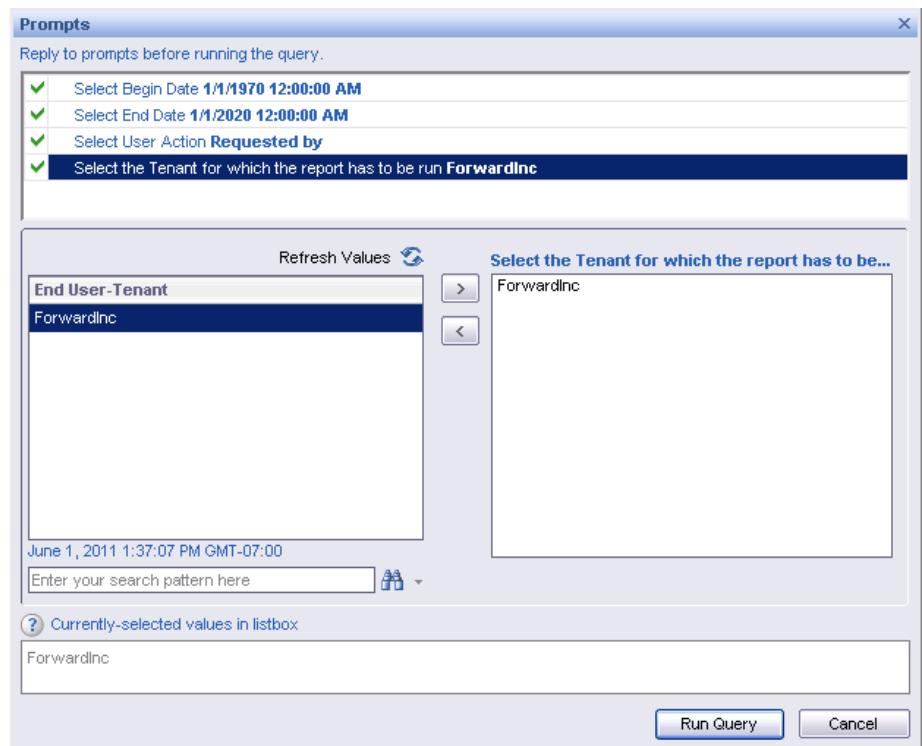
4. On the CA Service Catalog server, browse to the %USM_HOME%\reporting\CABI\ folder.
5. Open the TrustedPrincipal.conf file. Modify the following line so that the *shared secret* entered in the CMC is placed after the existing text. Save the file when done:
SharedSecret=
6. Restart the Service View service.

Verify the Integration

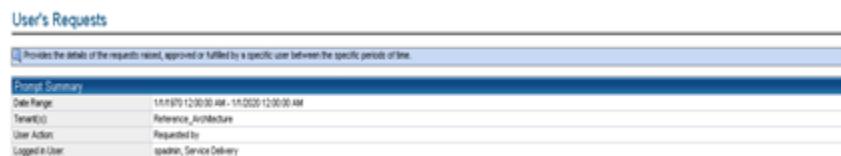
Follow these steps:

1. Log in to CA Service Catalog as a Service Delivery Administrator who has been authorized to view reports (that is spadmin).
2. Click the Reports link under the Home tab.
3. Click the InfoView button.
4. Click the Document List folder link.
5. Expand the following folders: Public Folders, CA Reports, CA SLCM.
6. Click the User Reports folder.
7. Right-click the User's Request report and click View.
The Prompts dialog opens.
8. Perform the following steps:
 - a. Select the row Select User Action.
 - b. Select Requested by and click the right arrow button (>).

- c. Select the row by the name Select the Tenant for which you run the report.
- d. Select the Service Provider tenant, and click the right arrow button (>).
- e. Click Run Query.



9. Verify that no errors occur.



Note: If the error message, No data to retrieve in Query in the report for the selected values appears, you can ignore it.

Integrate CA Business Intelligence with Active Directory

By integrating CA Business Intelligence with Active Directory you reduce the amount of user maintenance required in the user repository of BOXI.

Prerequisites for CA Business Intelligence Integration with Active Directory

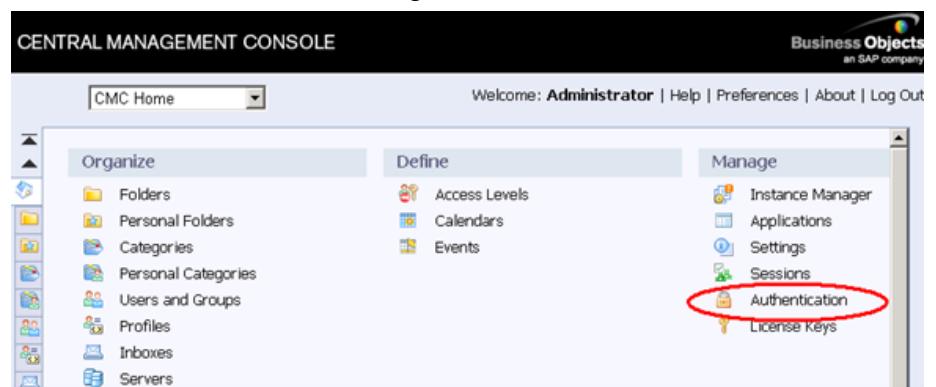
Verify the following items before you start the CA Business Intelligence integration with Active Directory:

- Verify that the CA Business Intelligence is installed, validated, and pass through the authentication that is configured according to the section, [How to Integrate CA Business Intelligence with CA Service Catalog](#) (see page 234).
- An Active Directory exists and (for best results) is populated with appropriate users and groups.
- CA EEM is installed and integrated with the Active Directory according to [Configure CA EEM for Active Directory](#).
- CA Process Automation and CA Service Catalog have been configured to use CA EEM for Authentication or Authorization.

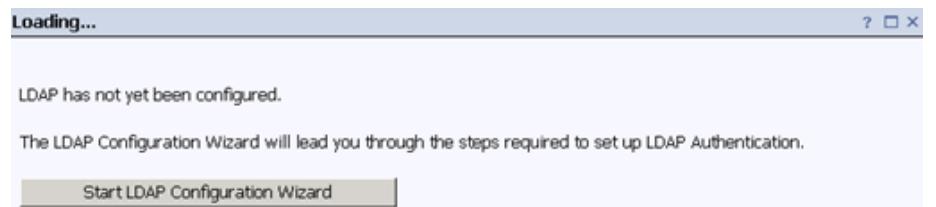
Configure CA Business Intelligence for LDAP Authentication

Follow these steps:

1. Click Start, All Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, BusinessObjects Enterprise Central Management Console.
2. Log in to the Central Management Console as the BOXI Application Administrator.
3. Click Authentication under the Manage column.



4. Double-click LDAP on the Authentication Page.
5. Click Start LDAP Configuration Wizard.



- Type the LDAP host name and Active Directory listening port, click Add, and click Next.

The screenshot shows a configuration interface for LDAP hosts. At the top, a header says 'LDAP'. Below it, a message says 'Please enter the LDAP hosts you are using.' There is a text input field 'Add LDAP host (hostname:port):' with a placeholder 'CARA-W2K8-DC01:389'. To the right of the input field are 'Add' and 'Delete' buttons. Below the input field is a list box containing 'CARA-W2K8-DC01:389'. At the bottom are 'Next >' and 'Cancel' buttons.

- Select the LDAP Server Type as Microsoft Active Directory Application, then click the Show Attribute Mappings link.

The screenshot shows a configuration interface for choosing an LDAP directory type. It says 'Choose the type of the LDAP directory you are using. You can customize the server parameters if required.' A dropdown menu 'LDAP Server Type:' shows 'Microsoft Active Directory Appl' selected. To the right is a link 'Show Attribute Mappings'. Below the dropdown are buttons '< Previous', 'Next >', 'Finish', and 'Cancel'.

The attribute mappings appear.

- Change the following attributes and click Next.

User Name

Value: sAMAccountName

Default User Search Attribute:

Value: sAMAccountName

Note: When the attributes are changed, the LDAP Server Type value changes to Custom automatically.

- Provide the Base LDAP Distinguished Name, and click Next.

For example, cn=users,dc=gsplab,dc=ca,dc=com

- Provide the Distinguished Name and password, leave the default for LDAP Credentials and Maximum Referral Hops, and click Next.

For example, CN=GSP

Admin,CN=Users,DC=GSPLAB,DC=ca,DC=com

- For the Type of SSL authentication, accept the default as Basic (no SSL) and click Next.

12. For Authentication, accept the default as Basic (no SSO) and click Next.

13. Set the appropriate LDAP Import options:

New Alias Options

- Assign each added LDAP alias to an account with the same name
- Create a new account for every added LDAP alias

Alias Update Options

- Create new aliases when the Alias Update occurs
- Create new aliases only when the user logs on

New User Options

- New users are created as named users
- New users are created as concurrent users

14. Click Finish.

15. Map LDAP Member Groups. Type the group name in the Add LDAP group (by cn or dn): Field, and click Add.

For example, cn=ForwardInc,cn=users,dc=gsplab,dc=ca,dc=com

Note: Do not prefix the LDAP group dn or cn with “secLDAP.”

Mapped LDAP Member Groups

Add LDAP group (by cn or dn):	<input type="text"/>	<input type="button" value="Add"/>
<input type="text" value="cn=ForwardInc,cn=users,dc=gsplab,dc=ca,dc=com"/>		<input type="button" value="Delete"/>

16. On the same screen, verify that the following options are selected:
 - **New Alias Options:**
Assign each added LDAP alias to an account with the same name.
 - **Alias Update Options:**
Create new aliases when the Alias Update Occurs.
 - **New User Options:**
New users are creates as concurrent users.
 - **Attribute Binding Options:**
 - Select the Import Full Name and Email Address checkbox.
 - Select the Give LDAP attribute binding priority over AD attribute binding checkbox.
17. Click Update to complete mapping.
 - a. Scroll to the top of the screen and verify the message, "LDAP Authentication updated" appears.
 - b. Close the screen and return to the Authentication screen in the Central Management Console.
18. Select Users and Groups from the Central Management Console drop-down list.

19. Verify that users are imported:
 - a. By default, the Group Hierarchy appears, showing the LDAP groups added in Step-14.
 - b. Click User List and verify that LDAP users are imported.
20. Add the mapped LDAP groups to the appropriate CA Business Intelligence groups by performing the following steps:
 - a. Click Group List. Right-click a group name and click "Add Members to Group".
 - b. Select the LDAP group, and click the ">" button.
 - c. Click OK.

Verify that the LDAP group shows up under the CABI group, under Group Hierarchy.

For example, map cn=Report Admins to the CA Report Admins group. In this example, the LDAP group members inherit privileges to administer reports.

Verify the Integration

Repeat the steps for [verifying the CA Business Intelligence integration with CA Service Catalog](#) (see page 249), logged in as a user authenticated through LDAP.

Note: The LDAP user must have appropriate CA Business Intelligence privileges to view a report. See the example in Step 19 of [Configure CA BI for LDAP Authentication](#) (see page 252) for one method of assigning privileges.

Configure CA IT Client Manager Software Delivery

Import Software Delivery Packages

Follow these steps:

1. Copy the Software Delivery Packages folder to CA IT Client Manager server.
2. Open DSM Explorer.
3. Expand asc-sql – Domain.
4. Expand Software.
5. Expand Software Packages Library.
6. Right-click Software Package Library, and select New, Software Group.
7. Enter a Name for the new Application Software Packages.
8. Click OK.
9. Right-click this new Application Software Package Group.
10. Select Import, Software Package.
11. Browser to the folder of each Software Package and highlight the reginfo folder.
12. Click Choose.
13. Verify that the correct Path appears in the Register Software Package window.
14. Check Source is on Manager.
15. Click OK.

The Package now appears under the new “Appliance” Software Group.
16. Continue importing Software Delivery Packages until all packages appear under the new “Appliance” Software Group.

Create a Software Delivery Package to deploy Batch Files

Perform the following procedures:

- [DPM Shutdown Action Package](#) (see page 258)
- [DPM Startup Action Package](#) (see page 259)

DPM Shutdown Action Package

DPM Shutdown Action Package

1. Click new software group.
2. Right-click New, Software Package.
 - Name – DPM Machine Shutdown
 - Version – 1.0
3. Click OK.
4. Expand the new package entry.
5. Click Software.
6. Right-click New volume, From Files.
 - Name – Shutdown
 - Source path
 - c:\DPM_shutdown_installer.bat
 - c:\DPM_shutdown_unistaller.bat
 - c:\DPM_shutdown_action.txt
7. Check Source is on Manager.
8. Click Procedures.
9. Right-click New, Procedure
 - Name – Install Action
 - Task – Install
 - Embedded File: DPM_shutdown_installer.bat; parameters: >
\$rf

10. Add second procedure
 - Procedures, New, External Procedure
 - Name – Activate Shutdown
 - Task – Activate
 - Embedded File: %WINDIR%\system32\shutdown.exe; parameters: -s -f

OR

 - File: %WINDIR%\system32\tsshutdwn.exe; parameters: /POWERDOWN
11. Add third procedure.
 - Procedures, New, Procedure
 - Name – Uninstall Action
 - Task – Uninstall
 - Embedded File: DPM_shutdown_uninstaller.bat; parameters: > \$rf

Seal the package before deployment.

To Deploy Software Package, DPM picks up automatically.

DPM Startup Action Package

Follow these steps:

1. Click new software group.
2. Right-click and choose New, Software Package.
 - Name – DPM Machine Startup
 - Version – 1.0
3. Click OK.
4. Expand the new package entry.
5. Click Software.
6. Right-click and choose New volume, From Files.
 - Name – Startup

- Source path

c:\DPM_startup_installer.bat

c:\DPM_startup_unistaller.bat

c:\DPM_startup_action.txt

c:\DPM_activate_action.bat

7. Check Source is on Manager.

8. Click Procedures.

9. Right-click and select New, Procedure.

- Name – Install Action

- Task – Install

- Embedded File: DPM_startup_installer.bat; parameters: > \$rf

10. Add second procedure.

- Procedures, New, Procedure

- Name – Activate Startup

- Task – Activate

- Embedded File: c:\DPM_activate_action.bat

11. Add third procedure

- Procedures, New, Procedure

- Name – Uninstall Action

- Task – Uninstall

- Embedded File: DPM_startup_unistaller.bat; parameters: > \$rf

Seal the package before deployment.

To Deploy Software Package, DPM picks up automatically.

Create a Software Delivery Package to Install an MSI Program

Follow these steps:

1. Click new software group.
2. Right-click and choose New, Software Package.
 - Name – Flash
 - Version – 9.0
3. Click OK.
4. Expand the new package entry.
5. Click Software.
6. Right-click and choose New volume, From Files.
 - Name – Flash.msi
 - Source path
c:\downloads\install_flash_player_active_x.msi
7. Check Source is on Manager.
8. Click Procedures.
9. Right-click and choose New, Procedure.
 - Name – Install
 - Task – Install
 - Embedded File: install_flash_player_active_x.msi
 - General - MSI method: install

Seal the package before deployment.

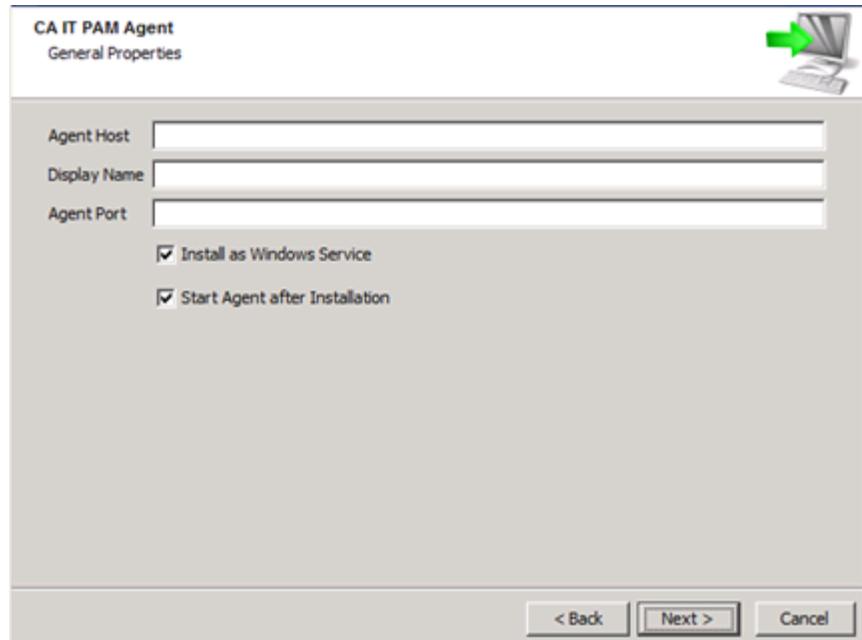
To Deploy Software Package, DPM picks up automatically.

CA IT Client Manager Installation and Configuration

Follow these steps:

1. Log in to the CA IT Client Manager and CA Server Automation server.
2. Install Java JDK.
3. Connect remotely to the CA Process Automation Manager.
4. Click Configuration, Installation palette.
5. Select Install Agent.
6. Click Install.
A message appears for you to run the application.
7. Click Run.
A Language Selection window opens.
8. Select English and click OK.
9. Click Next.
10. Select I accept the terms of the License Agreement, and click Next.
11. Browse to the Java Home Directory:
`C:\Program Files\Java\jdk1.7.0_51`
12. Click Next.
13. Verify the Destination Directory, and click Next.
14. Verify CA Process Automation Agent is the Start Menu.
15. Verify that Create shortcuts for all users is checked. Click Next.

16. Verify that the Domain URL points to the CA Process Automation Server. Click Next.



17. Verify that the Agent Host is the local server.
18. Verify that the Display Name is what you want.
19. Verify that the Agent Port is 7003.
20. Select the Install as Windows Service check box.
21. Select the Start Agent after Installation check box.
22. Verify the Scripts Temporary Directory.
23. Click Next. Click Finish.

Install Windows Automated Installation Kit

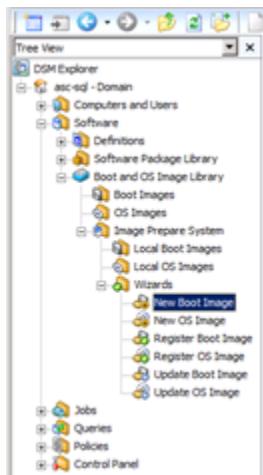
Follow these steps:

1. Copy Windows7AIK folder to CA IT Client Manager server.
2. Open and execute *STARTCD.EXE* using the Run as Administrator option.
3. Select Windows AIK Setup.
Welcome window appears.
4. Click Next.
5. Select I Agree, and click Next.
The Select Installation Folder window opens.
6. Verify or Browse to the Folder where Windows Automated Installation Kit is installed.
7. Verify that Everyone is selected, and click Next.
The Confirm Installation window opens.
8. Click Next.
The Installation Complete window opens.
9. Click Close, and Select Exit.

Create and Register Boot Images

Follow these steps:

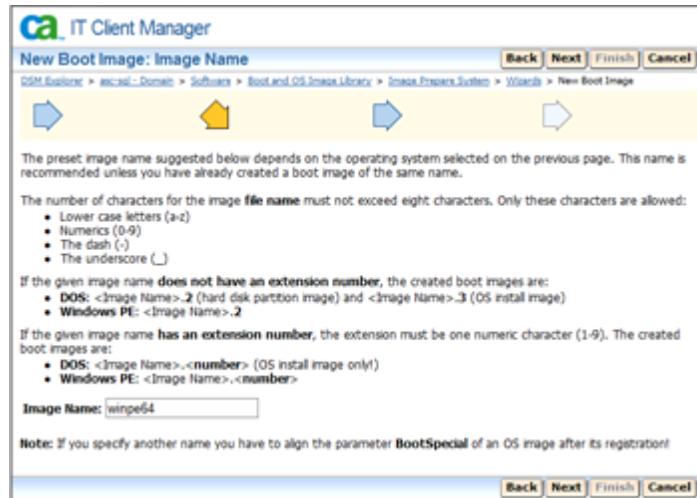
1. Open DSM Explorer.
2. Select the option In the future, do not show this dialog upon startup, and click Close.



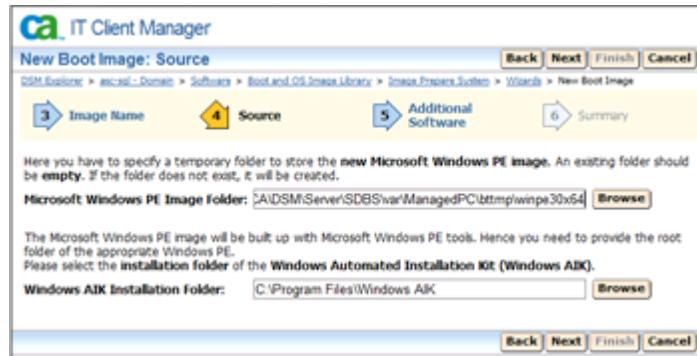
3. Expand Software, Boot and OS Image Library, Image Prepare Systems, Wizards, New Boot Image.
4. Click Next.
5. Select WINPE30.
6. Select Create Microsoft Windows PE Image and click Next.
7. Change the Image Name as *winpe32* and click Next.
8. Verify or Browse to change the Microsoft Windows PE Image Folder.
9. Verify or Browse to change the Windows AIK Installation Folder.
10. Click Next.
11. Verify that Default Windows PE Boot Loader file is selected and that pxeboot.n12 is the value.
12. Click Next.
13. Click Finish.

This process can take about five minutes to complete.

14. Click Run Wizard.
15. Select WINPE30x64 and click Next.



16. Change the Image Name as winpe64 and click Next.



17. Verify or Browse to change the Microsoft Windows PE Image Folder (default okay).
18. Verify or Browse to change the Windows AIK Installation Folder.

19. Click Next.



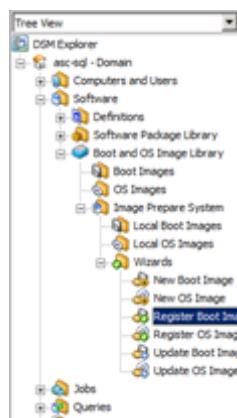
20. Verify that Default Windows PE Boot Loader file is selected and that pxeboot.n12 is the value.

21. Click Next.

22. Click Finish.

The command finished successfully message opens.

23. Click OK.

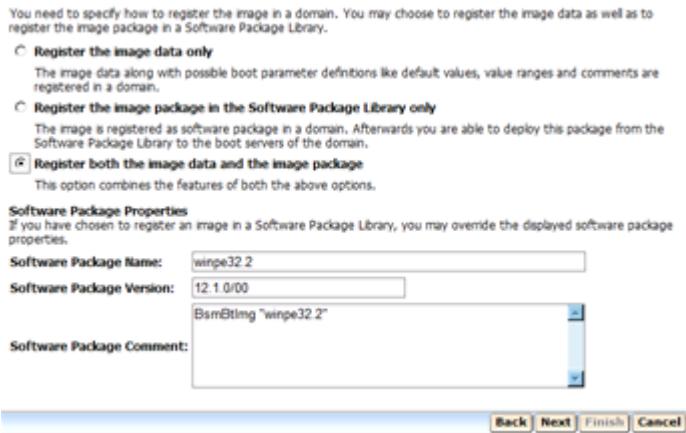


24. Select Register Boot Image, and click Next.

25. Verify that Register locally created Boot Image is selected.

26. Select the new Boot Image (winpe32.2).

27. Click Next.



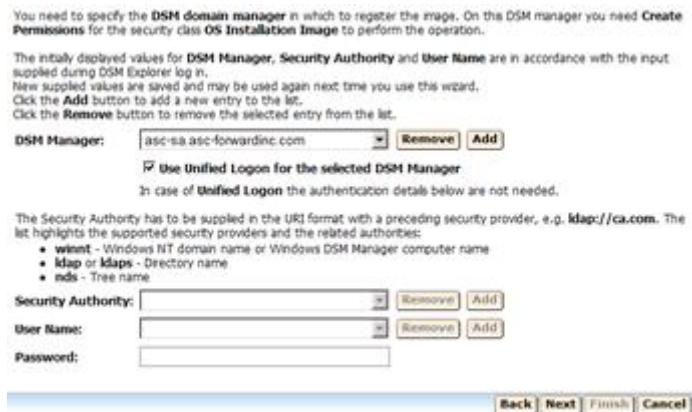
28. Verify Register both the Image data and the Image package is selected.

29. Verify the Software Package Name.

30. Verify the Software Package Version.

31. Verify the Software Package Comments.

32. Click Next.



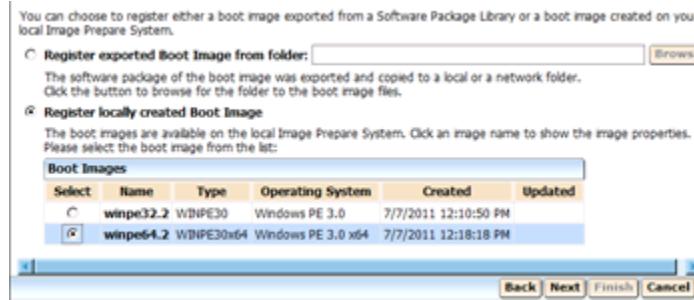
33. Verify the DSM Manager is correct.

34. Verify that Use Unified Logon for the selected DSM Manager is selected.

35. Click Next.

The Register Boot Image Summary window opens.

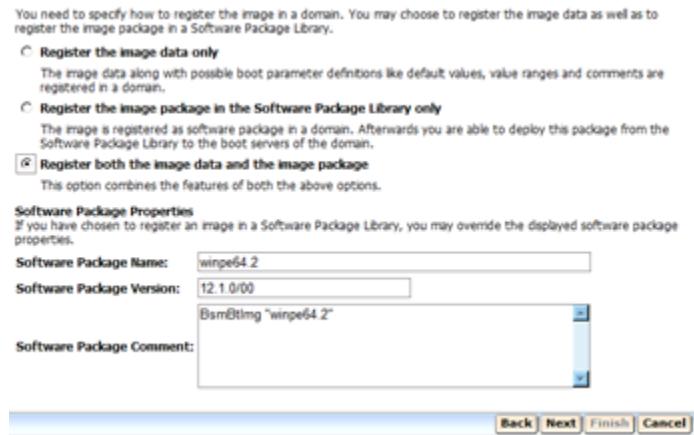
36. Click Finish.
37. Verify and wait until the “Command finished successfully” opens.
38. Click Run Wizard.



39. Verify that Register locally created Boot Image is selected.

40. Select the new Boot Image (winpe64.2).

41. Click Next.



42. Verify Register both the Image data and the Image package is selected.

43. Verify the Software Package Name.

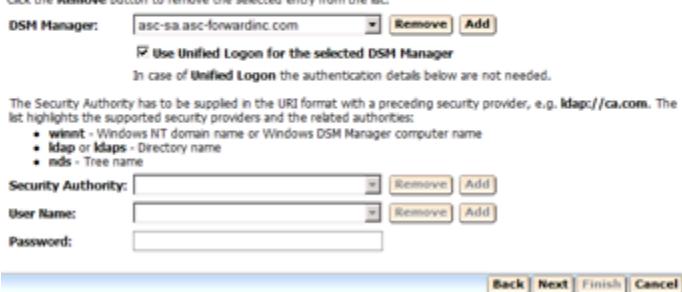
44. Verify the Software Package Version.

45. Verify the Software Package Comments.

46. Click Next.

You need to specify the **DSM domain manager** in which to register the image. On this DSM manager you need **Create Permissions** for the security class **OS Installation Image** to perform the operation.

The initially displayed values for **DSM Manager**, **Security Authority** and **User Name** are in accordance with the input supplied during DSM Explorer log in.
New supplied values are saved and may be used again next time you use this wizard.
Click the **Add** button to add a new entry to the list.
Click the **Remove** button to remove the selected entry from the list.



47. Verify that the DSM Manager is correct.

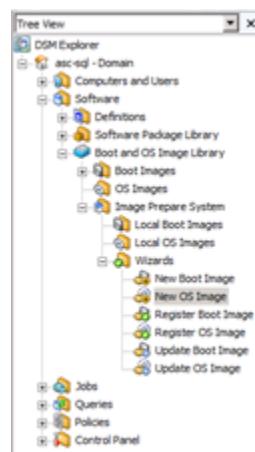
48. Verify that Use Unified Logon for the selected DSM Manager is selected.

49. Click Next.

50. Click Finish.

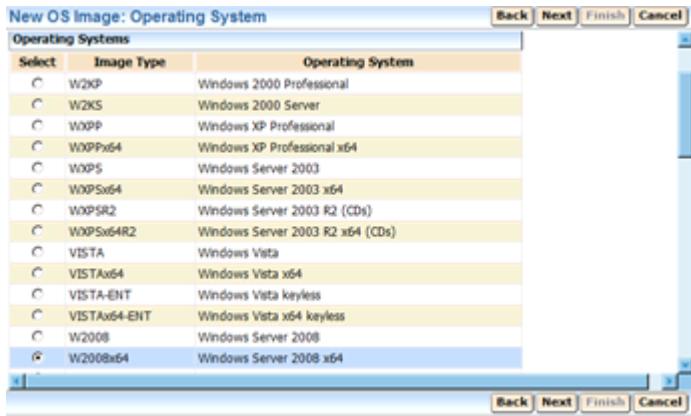
Verify and wait until the “Command finished successfully” opens.

51. Click OK.



52. Select New OS Image.

53. Click Next.

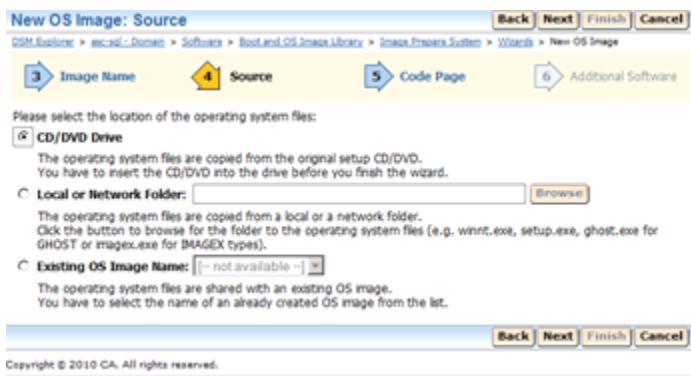


54. Select the Operating System that you wish to add (Windows Server 2008 x64).

55. Click Next.

56. Enter an Image Name (w2k8-64).

57. Click Next.

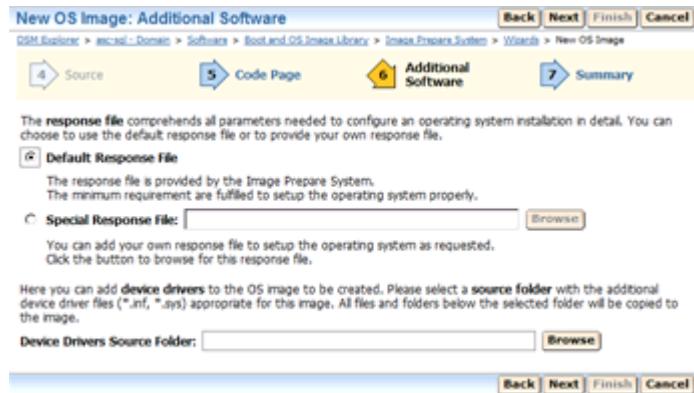


58. Select CD/DVD Drive, Local or Network Folder, or Existing OS Image Name and link to the Operating System Image files.

59. Click Next.

60. Verify 1252 - Western European is selected.

61. Click Next.



62. Verify that Default Response File is selected.

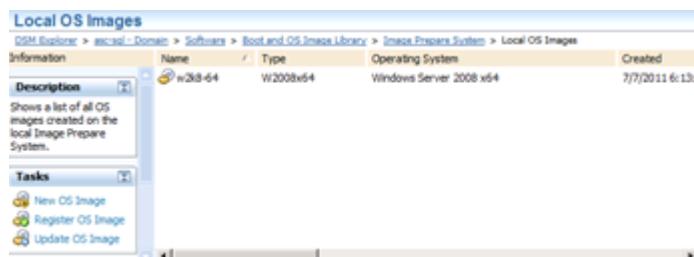
63. Click Next.

64. Verify the Summary information.

65. Click Finish.

If CD/DVD was selected for the Operating System, then you will be prompted to load media and click Continue, for each is disk or ISO image.

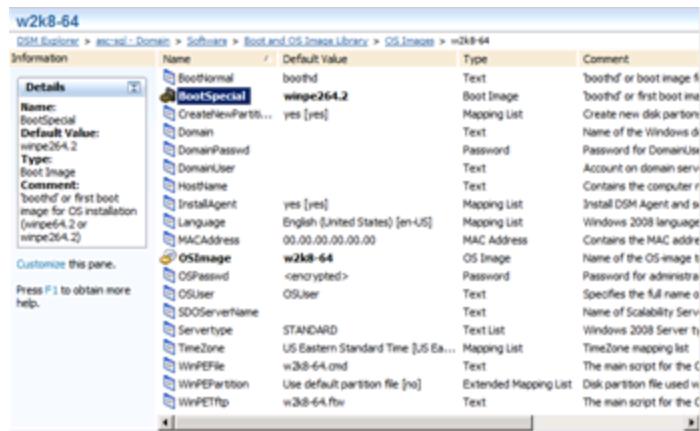
66. Click OK.



67. Verify that the Local OS Images is highlighted.

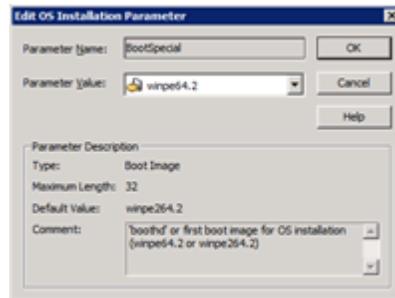
68. Right-click the new OS Image (w2k8-64).

69. Select Register OS Image in Connected Domain, Data and Software Package.
70. Click OK.
71. Expand OS Images.
72. Highlight the new OS Image (w2k8-64).



Name	Default Value	Type	Comment
bootNormal	bootfd	Text	'bootfd' or boot image file
bootSpecial	winpe64.2	Boot Image	'bootfd' or first boot image for OS installation (winpe64.2 or winpe264.2)
createNewPartitions	yes [yes]	Mapping List	Create new disk partitions
domain		Text	Name of the Windows domain
domainPasswd		Password	Password for Domain\
domainUser		Text	Account on domain server
hostName		Text	Contains the computer name
installAgent	yes [yes]	Mapping List	Install DSM Agent and services
language	English (United States) [en-US]	Mapping List	Windows 2008 language
macAddress	00:00:00:00:00:00	MAC Address	Contains the MAC address
osImage	w2k8-64	OS Image	Name of the OS-image to install
osPassword	<encrypted>	Password	Password for administrator
osUser	OSUser	Text	Specifies the full name of the user
sdsServerName		Text	Name of Scalability Server
serverType	STANDARD	Text List	Windows 2008 Server type
timeZone	U.S. Eastern Standard Time [US Eastern Daylight Time]	Mapping List	TimeZone mapping list
winPEFile	w2k8-64.cmd	Text	The main script for the OS
winPEPartition	Use default partition file [no]	Extended Mapping List	Disk partition file used with the OS
winPETHlp	w2k8-64.fbw	Text	The main script for the OS

73. Right-click BootSpecial and select Edit Default Value.



74. From the drop-down list change the Parameter Value to the correct Boot Image created earlier (winpe64.2).
75. Click OK.
76. Close the DSM Explorer.

Chapter 5: Upgrade to the Current Release

The new users can directly install CA Automation Suite for Clouds Release 1.7.1 as it contains complete content. Installation of earlier version of CA Automation Suite for Clouds is not required.

Upgrade in both the scenarios must be done as follows:

1. Upgrade the products.
2. Upgrade Foundation Console.
3. Upgrade CA ASC Server Automation-ESX content.

Depending on your existing environment, perform the steps provided in *one* of the following sections to upgrade to current release of CA Automation Suite for Clouds Base Configuration.

- [Upgrade from CA Automation Suite for Clouds Base Configuration 1.7](#) (see page 275).
- [Upgrade from CA Automation Suite for Clouds Base Configuration 1.6 SP01](#) (see page 290).

Upgrade from Release 1.7

In this scenario, you upgrade all products associated with CA Automation Suite for Clouds Base Configuration Release 1.7.1 first, and then the content. For information on upgrading the individual products, see the respective product documentation.

The following table provides the supported product version details of Release 1.7 and the current release:

Product Name	Supported Product Version for Release 1.7	Supported Product Version for Release 1.7.1
CA Service Catalog	r12.8 CP02 with RO65483, RO65485, and RO65486 patches	r12.8 CP03 with RO70135 patch
CA Process Automation	r4.1 SP1	r4.1 SP1 or r4.2 SP1
CA EEM	r12.0.7.57	r12.5 CR1
CA Server Automation	r12.8.1	r12.8.2
CA Business Intelligence	r3.3	r3.3

When you upgrade the content pack some services, service options group and forms are affected; in some cases report objects or plugins are modified.

Perform the following procedures to upgrade:

1. [Review the Prerequisites](#) (see page 276).
2. Upgrade CA EEM.
3. Upgrade CA Process Automation.
4. Upgrade CA Server Automation.
5. [Apply CA Service Catalog Patches](#) (see page 276).
6. [Upgrade Content](#) (see page 277).
7. [Post Upgrade Configuration](#) (see page 283).

Review the Prerequisites

Verify the following prerequisites before you begin the upgrade:

- Set the environment variable for CA EEM on the CA Server Automation server.

Important! Solution upgrade is not supported if CA EEM and CA Server Automation are installed on the same server.

To set the environment variable, open the System Properties, Advanced, Environment Variables. Click System variables, New, and set the variable name as CA_ALLOW_UNSUPPORTED_EEM and Variable value to True.

Apply CA Service Catalog Patches

To enable CA Service Catalog to work with CA Automation Suite for Clouds, apply the CA Service Catalog r12.8 CP 3 and RO70135 patches to your installation.

Follow these steps:

1. Log in to <https://ca.com/support> with your credentials.
2. Click Download Center, search for and download the following patches:
 - CP03
 - RO70135
3. Extract the zip files.
4. Follow the instructions mentioned in the patch installation readme.

The patch is applied.

You have successfully completed installing CA Service Catalog and the required patches.

Upgrade Content

This section details the upgrade procedures for CA Automation Suite for Clouds Foundation and CA Automation Suite for Clouds Base Configuration content.

1. [Upgrade CA Automation Suite for Clouds Foundation Content](#) (see page 277).
2. [Upgrade CA Automation Suite for Clouds Base Configuration ESX Content](#) (see page 281).

Upgrade CA Automation Suite for Clouds Foundation Content

This section details the content upgrade procedures for CA Automation Suite for Clouds Foundation.

Review Prerequisites

Complete and verify the following items before you start upgrading the CA Automation Suite for Clouds Foundation:

- Back up all user data, groups, and other related items.
- Verify ASC_Security_GlobalDataset is checked in and closed.
To verify, open the CA Process Automation client that is configured with existing CA Automation Suite for Clouds. Navigate to Default Environment: Orchestrator. If ASC_Security_GlobalDataset is checked out and open, check in and close. If the data set is in the checked out state, upgrade can fail to update the data set.
- Ensure that the latest patches are installed on the CA Service Catalog server.

Upgrade Content

Before you start upgrading, rename all the existing folders under the content packs folder with a suffix, _old. This step prevents conflict among the new files that you are going to deploy.

Follow these steps:

1. Unzip *CA ASC Base Foundation.zip* contents from the media to the %USM_HOME%/filestore/contentpacks folder.
2. Open the CA Service Catalog Command Prompt window, change directory to: %USM_HOME%/filestore/contentpacks/CA ASC Base Foundation.
3. Copy the securityrealm folder that is under the CA ASC Foundation to the CA Process Automation server.
4. Run *DeployBaseConsole.cmd*.

5. Type the tenant ID at the following prompt.

Enter the id of the tenant you want to import the content pack into (Required):

Note: The tenant ID is case-sensitive.

For example, Forward Inc.

The installer automatically detects the existing version of the base model in your environment, the following message appears:

6. Type y to continue to upgrade at the following prompt.

A previous version of CA ASC Foundation is detected, do you want to upgrade to ASC 1.7.1? Press y to upgrade or any key to exit the setup:

Note: If an existing installation is not detected, the installation of CA Automation Suite for Clouds Base Configuration Release 1.7.1 proceeds.

On successful upgrade, BUILD SUCCESSFUL message appears.

If the build has failed, press any key other than 'y' to exit the setup.

7. Press Enter at the following prompt.

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

8. Type y to continue at the following prompt.

Installation will re-start CA Service Catalog multiple times. Please press y to continue or any key to exit: y

9. Press Enter at the following prompt.

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

10. Type the database credentials to configure ASC schema at the following prompts.

Enter Service Catalog Database Administrator (Default sa):

Enter Service Catalog Database Administrator Password:

11. Type y at the following prompt to proceed creating groups.

If build is successful, enter y to Create Groups or any key to exit the setup:

Following groups are created in CA EEM and assigns permissions to the service offerings in CA Service Catalog as defined in the content pack groups properties file:

- ASCgrp_baseconsole_NormalUser
- ASCgrp_baseconsole_Admin

Note: The groups in CA EEM are used for the *Request user to Service group* offering. All the permissions that are assigned in CA Automation Suite for Clouds before upgrade remain unchanged. The CA EEM groups and permissions are in addition to the existing Active Directory groups and set of permissions.

Verify Default Rules

Ensure that the following sets of default CA Service Catalog rules that you disabled during the content deployment are still disabled:

Following rules are located under Request/Subscription item change.

- When Status is Submitted and Approval Process is driven by Workflow.
- When Status is Pending Approval and Requested By and Requested For users are different.
- When Status is Pending Approval.
- When Status is Fulfillment Canceled.
- When Reservation Request is Rejected.
- When Reservation Request is Approved.
- When Status is Pending Fulfillment.

Following rules located under Request Pending action item change.

- When action is Canceled.
- When action is Delegated.
- When action is Returned.
- When action is Taken.
- When action is Transferred
- When Fulfilled.
- When Pending Approval actions are Assigned.
- When Pending Approval actions are Assigned and Requested By and Requested For users are different.
- When Pending Fulfillment actions are Completed.
- When Status is Approved.
- When Status is Rejected.
- When Pending Fulfillment actions are Assigned.

Verify Datasets

After you deploy the upgrade, verify the following dataset in CA Process Automation:

- ASC_Security_GlobalDataset
 - Login Parameters CHANGE ME
 - APP URLs CHANGE ME
 - AD Parameters CHANGE ME
 - EEM Parameters

Verify Upgrade

Verify the upgrade by performing the following steps:

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, and Content Packs.

Content packs installed before and after CA Automation Suite for Clouds upgrade appears.

3. Verify that names and ID after upgrade appears correctly.
4. Verify that all users are available and you are able to log in to CA Service Catalog.
5. Verify that the users created using the User Onboarding procedure are available.

After you complete upgrading the CA Automation Suite for Clouds Foundation, continue upgrading the CA Automation Suite for Clouds Base Configuration for ESX deployed in your environment.

Upgrade CA Automation Suite for Clouds Base Configuration ESX Content

This section details the content upgrade procedures for CA Automation Suite for Clouds Base Configuration for ESX.

Review Prerequisites

Complete and verify the following items before you start upgrading the ESX content pack for CA Automation Suite for Clouds Base Configuration:

- Verify that CA Automation Suite for Clouds Foundation upgrade is complete.
- Make sure that ASC_Security_GlobalDataset is checked in and closed.

To verify, open the CA Process Automation client that is configured with existing CA Automation Suite for Clouds. Navigate to Default Environment: Orchestrator. If ASC_GlobalDataset is checked out and open, check in and close. If the data set is in the checked out state, upgrade can fail to update the data set.

Upgrade Content

Before you start upgrading, rename all the existing folders under the content packs folder with a suffix, _old. This step prevents conflict among the new files that you are going to deploy.

Follow these steps:

1. Unzip *CA ASC Server Automation - ESX.zip* contents from the media to %USM_HOME%/filestore/contentpacks.
2. Open a CA Service Catalog Command Prompt window, change directory to %USM_HOME%/filestore/contentpacks/CA ASC Server Automation - ESX.
3. Run *DeployServerAutomation-ESX.cmd*.
4. Type the tenant ID at the following prompt.

Enter the id of the tenant you want to import the content pack into (Required):

Note: The tenant ID is case-sensitive.

For example, Forward Inc.

The Installer automatically detects the existing version of the content pack in your environment, the following message appears:

5. Type y to continue to upgrade.

An earlier version of CA ASC SA ESX Cartridge is detected, do you want to upgrade to ASC 1.7.1? Press y to upgrade or any key to exit the setup:

If an existing installation is not detected, the installation of CA Automation Suite for Clouds Base Configuration Release 1.7.1 proceeds.

6. Type y at the following prompt to proceed with upgrade.

Installation will re-start CA Service View multiple times. Please press y to continue or any key to exit:

On successful upgrade, the BUILD SUCCESSFUL message appears.

If the build fails, enter any key other than y to exit the setup.

7. Press Enter at the following prompt.

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

8. Type the database credentials to configure ASC schema at the following prompts.

Enter Service Catalog Database Administrator (Default sa):

Enter Service Catalog Database Administrator Password:

9. Type y at the following prompt to proceed creating groups.

If build is successful, enter y to Create Groups or any key to exit the setup:

After the groups are successfully created, the following message opens.

Offering permissions set successfully in CA Service Catalog.

The following groups are created in CA EEM and assigns permissions to the service offerings in CA Service Catalog as defined in the content pack groups properties file:

- ASCgrp_sa_esx_Snapshots
- ASCgrp_sa_esx_DataStore
- ASCgrp_sa_esx_Reservation_Create
- ASCgrp_sa_esx_Reservation_Extend
- ASCgrp_sa_esx_Reservation_Return
- ASCgrp_sa_esx_Reservation_Change

Note: The newly created groups in CA EEM are used for the *Request user to Service group* offering. All the permissions and groups that are created in CA Automation Suite for Clouds before upgrade remain unchanged. The new groups and permissions are in addition to the existing set of permissions and groups.

Verify Datasets in CA Process Automation

After you deploy the CA Automation Suite for Clouds Base Configuration for ESX upgrade, verify the following datasets in CA Process Automation:

- ASC_GlobalDataset under the CA ASC folder.
 - Login Parameters
 - APP URLs CHANGE ME

Verify Upgrade

Verify the upgrade by performing the following steps:

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, and Content Packs.
Content packs installed before and after CA Automation Suite for Clouds upgrade appears.
3. Verify that names and ID after upgrade appears correctly.

You have completed the CA Automation Suite for Clouds Base Configuration for ESX upgrade. All content packs are upgraded for CA Automation Suite for Clouds Release 1.7.1.

Post Upgrade Configuration

After you upgrade all products and content perform the following steps to complete the upgrade:

- [Configure Super User on CA Server Automation](#) (see page 283).
- [Configure CA Process Automation Datasets for ESX](#) (see page 199).

Configure Super User on CA Server Automation

Perform the following procedure to enable the ability for multiple users to manage the reservations lifecycle.

Follow these steps:

1. Log in to the CA Server Automation server.
2. Open a Command Prompt window, change directory to:
C:\CA\ServerAutomation\bin

3. Run the following command:

```
dpmutil -set --super
```

4. Type the CA EEM credentials at the prompt.

5. Type 1 at the following prompt:

Enter the number for one of the following, or press enter for default:

6. Type the System Administrator credentials.

On the successful configuration, the Configuration finished successfully message appears. You have completed setting the set super user.

7. Run the following command:

```
dpmutil -get --super
```

8. Type the CA EEM Administrator credentials at the prompt.

The Administrator username and platform details are displayed.

On the successful verification, the Configuration finished successfully message appears again. You have verified the super user configuration.

Configure CA Process Automation Datasets for ESX

Configure the CA Process Automation datasets to provide data to the CA Automation Suite for Clouds Base Configuration automated processes for ESX. For more information about datasets, see the CA Process Automation documentation.

Note: Configure *Error Handling Parameters* in ASC_GlobalDataset and then proceed configuring the datasets that are listed in this topic.

The Datasets capture information of CA Server Automation and Reservation Manager Host, port, userid, and password to connect to CA Server Automation. These details help in provisioning, changing, and snapshot features. In addition, datasets also capture CA Service Catalog, CA Process Automation host, and login credentials to initiate the web services. These details help the solution to get the information from CA Service Catalog and update the request states.

Follow these steps:

1. Log in to the CA Process Automation console.
2. Click the Library tab from the home page.
3. Click the CA ASC folder.
4. Click ASC_GlobalDataset and Check Out.

Note: Delete all the unwanted or unused dataset values to ensure proper connection.

5. Click Login Parameters CHANGE ME and complete the following details:

userID

Specifies the CA Service Catalog Administrator user name.

Value: spadmin

password

Specifies the CA Service Catalog Administrator password.

businessUnit

Specifies the CA Service Catalog business unit name (This value is case-sensitive).

SAM_User

Specifies the CA Server Automation Administrator user name.

SAM_Password

Specifies the CA Server Automation Administrator password.

SpecAM_Touchpoint

If the CA Process Automation Agent is installed on CA Server Automation, then enter the Touchpoint value. This information is used for the datastore and VMware ESX provisioning.

6. Click APP URLs CHANGE ME and complete the following details:

SLCM_URL

Specifies the CA Service Catalog URL.

ITPAM_URL

Specifies the CA Process Automation URL.

SAM_URL

Specifies the CA Server Automation URL.

7. Click Misc Parameters CHANGE ME and complete the following details:

Administrator_Email

Specifies the administrator email.

VC_ESX_HostName

Specifies the ESX host name. This information is used in VMware ESX provisioning.

VC_Datacenter_Name

Specifies the Datacenter name. This information is used in VMware ESX provisioning.

VC_Server_Name

Specifies the vCenter server name. This information is used in VMware ESX provisioning.

SpecAM_Home

Specifies the CA Server Automation bin folder path. This information is used in VMware ESX provisioning.

SpecAMTouchpoint

Specifies the SpecAM Touchpoint. If the CA Process Automation Agent is installed on the CA Server Automation server, then enter the Touchpoint value. This information is used for the datastore and VMware ESX provisioning.

ESX_HostUser

Specifies the ESX host user name. This information is used in VMware ESX provisioning.

Value: root

ESX_OperationRetry

Specifies the retry count, when the operation fails.

Default: 3

ESX_WaitAttempts

Specifies the number of attempts during the wait period.

Default: 5

ESX_WaitTime

Specifies the time interval between each attempt.

Default: 60

StorageAdminOrAdminGroup

Specifies the storage admin.

WindowsAdmin

Specifies the Windows VM template parameters.

Specify the AdminPassword value for the default template. This value is used when the template is not available in the valuemap. Continue creating index values for each Windows VM Template:

Expand the Windows Admin folder, add Indexed Value. A new parameter set is added.

Expand Parameters, and add the following values:

Template

Specifies the name of the Windows virtual machine template.

AdminUserName

Specifies the user name of the virtual machine that accesses the newly provisioned Windows VM using the template.

Default: administrator

AdminPassword

Specifies the administrator password.

IsPasswordProvided

Specifies whether password is provided or not.

Change the parameter value to True if the password is provided.

Default: False

LinuxAdmin

Specifies the Linux VM template parameters.

Specify the AdminPassword value for the default template. This value is used if the template is not available in the valuemap. Continue creating index values for each Linux VM Template:

Expand the LinuxAdmin folder, Add Indexed Value. A new parameter set is added.

Expand Parameters, and add the following values:

Template

Specifies the name of the Linux virtual machine template.

AdminUserName

Specifies the user name of the virtual machine that accesses the newly provisioned Linux VM using the template.

Default: root

AdminPassword

Specifies the administrator password.

SSHPort

Specifies the port where SSH service is listening on the newly provisioned Linux virtual machine with the template.

Default: 22

UseSudo

Specify true if you want to use the sudo user in the Linux environment. For information about configuring the sudo user, see the [Update the sudoers File](#) (see page 207) section.

IsPasswordProvided

Specifies whether password is provided or not.

Change the parameter value to True if password is provided.

Default: False

PAMHome

Specifies the CA Process Automation installation path.

Example: C:\Program Files (x86)\CA\PAM

StorageOwner

Specifies the name of storage server that is configured with CA Server Automation.

8. Click *AD Login Parameters* CHANGE ME and complete the following details:

Adding these parameters allows you to toad secondary users as local administrator to the provisioned machine.

domainName

name of domain

Example: ca

domainAdmin

Specifies the domain administrator name.

domainAdminPassword

Specifies the domain administrator password.

isDomainAdminPasswordProvided

Specifies whether domain administrator password is provided or not.

Change the parameter value to True if the password is provided.

Default: False

9. Click Pam Parameters CHANGE ME and complete the following details:

pamMachineAdmin

Specifies the CA Process Automation machine administrator user name.

Default: Administrator

pamMachineAdminPassword

Specifies the CA Process Automation machine administrator password.

10. Click Storage and enter the details of the following storage services.

Note: If Storage is configured, highlight the Storage Value Definition for the storage integration.

- storageSpecAMTouchpoint
- storageSpecAM_Host_Admin
- storageSpecAM_Host_Password
- storageTierBronzeLabel
- storageTierSilverLabel
- storageTierGoldLabel

Note: If the CA Process Automation Agent has been installed on CA Server Automation, then enter the Touchpoint in the SpecAM_Touchpoint field.

11. Click Save.
12. Click Check In.
13. Close ASC_GlobalDataset.

You have configured the CA Process Automation content for CA Automation Suite for Clouds Base Configuration for ESX.

Upgrade from Release 1.6 SP01

In this scenario, you upgrade all products associated with CA Automation Suite for Clouds Base Configuration Release 1.6 SP01 first, and then the content. For information on upgrading the individual products, see the respective product documentation.

The following table provides the supported product version details of Release 1.6 SP01 and the current release:

Product Name	Supported Product Version for CA Automation Suite for Clouds Release 1.6 SP01	Supported Product Version for Release 1.7.1
CA Service Catalog	r12.7 with RO60036 (CP05) and RO60274 patches or r12.8 with RO58569 (CP01) and RO60273 patches	r12.8 CP03 with RO70135 and RO65483 patches
CA Process Automation	r4.0 SP1 CP02 or r4.1 SP1	r4.1 SP1 or r4.2 SP1
CA EEM	r8.4 or r12.0.7.57	r12.5 CR1
CA Server Automation	r12.8	r12.8.2
CA Business Intelligence	r3.3	r3.3

When you upgrade the content pack some services, service options group and forms are affected; in some cases report objects or plugins are modified.

Perform the following procedures to upgrade:

1. [Review the Prerequisites](#) (see page 291).
2. Upgrade CA EEM.
3. Upgrade CA Process Automation.
4. Upgrade CA Server Automation.
5. [Upgrade CA Service Catalog](#) (see page 292).
6. [Apply CA Service Catalog Patches](#) (see page 276)
7. [Upgrade Content](#) (see page 277).
8. [Post Upgrade Configuration](#) (see page 301).

Review the Prerequisites

Verify the following prerequisites before you begin the upgrade:

- Set the environment variable for CA EEM on the CA Server Automation server.
Important! Solution upgrade is not supported if CA EEM and CA Server Automation are installed on the same server.

To set the environment variable, open the System Properties, Advanced, Environment Variables. Click System variables, New, and set the variable name as CA_ALLOW_UNSUPPORTED_EEM and Variable value to True.

Access the Published Service Offering in CA Service Catalog r12.7

The published service offering in CA Service Catalog r12.7 is sometimes not accessible by default. You must request or subscribe to the service offering to access them.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Service Offerings, Offerings.
3. Select a published service offering from the left menu.
4. Click Permissions tab, Groups.
5. Select the groups to grant permission.
6. Click Save.

You can access the published services.

Upgrade CA Service Catalog

Apply patches on CA Service Catalog 12.8 environment.

Review Prerequisites to Upgrade CA Service Catalog

The following patch is required to upgrade CA Service Catalog:

- RO65483

Follow these steps:

1. Log in to <https://ca.com/support> with your credentials.
2. Click Download Center, search for and download the patches.

You have the required patches to upgrade CA Service Catalog.

Upgrade CA Service Catalog

Perform the following steps to upgrade CA Service Catalog.

Follow these steps:

1. Log in to the existing CA Service Catalog server as an administrator.
2. [Upgrade CA Service Catalog](#) (see page 136).
On successful upgrade, the installer prompts you to run the setup utility.
3. [Run Setup Utility](#) (see page 141).
4. [Configure the Database Module](#) (see page 143).
5. [Configure the Security Module](#) (see page 146).
6. Run the SQL query `configureMSSQLMDB.sql` on MDB.
The SQL query is available in patch RO65483.
Important: Ensure that you run the SQL query, after configuring the security module and before configuring the components module of Setup Utility.
7. [Configure the Components Module](#) (see page 148).

You have successfully completed CA Service Catalog upgrade.

Apply CA Service Catalog Patches

To enable CA Service Catalog to work with CA Automation Suite for Clouds, apply the CA Service Catalog r12.8 CP 3 and RO70135 patches to your installation.

Follow these steps:

1. Log in to <https://ca.com/support> with your credentials.
2. Click Download Center, search for and download the following patches:
 - CP03
 - RO70135
3. Extract the zip files.
4. Follow the instructions mentioned in the patch installation readme.

The patch is applied.

You have successfully completed installing CA Service Catalog and the required patches.

Update CA Service Catalog Content

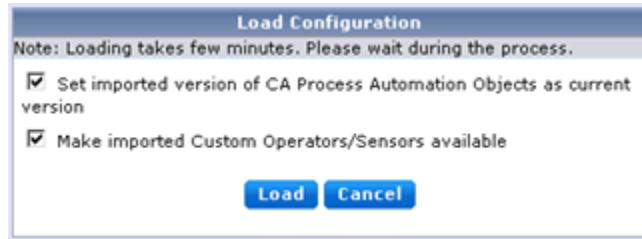
Perform the following steps to upgrade CA Service Catalog content.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.
2. Click Administration, Configuration.
3. Click CA Process Automation.

CA Process Automation Configurations		Add	Delete		
Order of configuration: Load > Configure > Test		Launch	Load	Configure	Test
Property	Value	Modify			
Certificate File Path on CA Process Automation	Not Configured				
Enable Automatic Retry	Yes				
Enable HTTPS	No				
Host Name					
Key File Path on CA Process Automation	Not Configured				
Password for Certificate on CA Process Automation	Not Configured				
PEM Certificate File Name	ITPAMCertfile.pem				
Port Number (1-65535)	8080				
Retry Count (0-10)	3				
Retry Interval (0-3600) (in secs.)	15				
Use Certificate for Authentication	No				
User ID	pamadmin				
User Password	*****				

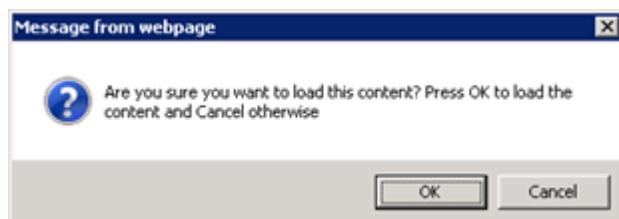
4. Click Load in the upper right corner.



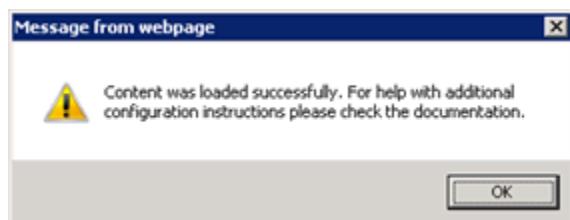
5. Complete the following settings:

- Select Set imported version of CA Process Automation Objects as current version.
- Select Make imported Custom Operators/Sensors available.

6. Click Load.



7. Click OK.



8. Click OK, when the content has successfully loaded.

9. Click Configure in the upper right corner.



10. Click OK.

You have successfully updated the required content.

Upgrade Content

This section details the upgrade procedures for CA Automation Suite for Clouds Foundation and CA Automation Suite for Clouds Base Configuration content.

1. [Upgrade CA Automation Suite for Clouds Foundation Content](#) (see page 277).
2. [Upgrade CA Automation Suite for Clouds Base Configuration ESX Content](#) (see page 281).

Upgrade CA Automation Suite for Clouds Foundation Content

This section details the content upgrade procedures for CA Automation Suite for Clouds Foundation.

Review Prerequisites

Complete and verify the following items before you start upgrading the CA Automation Suite for Clouds Foundation:

- Back up all user data, groups, and other related items.
- Verify ASC_Security_GlobalDataset is checked in and closed.
To verify, open the CA Process Automation client that is configured with existing CA Automation Suite for Clouds. Navigate to Default Environment: Orchestrator. If ASC_Security_GlobalDataset is checked out and open, check in and close. If the data set is in the checked out state, upgrade can fail to update the data set.
- Ensure that the latest patches are installed on the CA Service Catalog server.

Upgrade Content

Before you start upgrading, rename all the existing folders under the content packs folder with a suffix, _old. This step prevents conflict among the new files that you are going to deploy.

Follow these steps:

1. Unzip *CA ASC Base Foundation.zip* contents from the media to the %USM_HOME%/filestore/contentpacks folder.
2. Open the CA Service Catalog Command Prompt window, change directory to: %USM_HOME%/filestore/contentpacks/CA ASC Base Foundation.
3. Copy the securityrealm folder that is under the CA ASC Foundation to the CA Process Automation server.
4. Run *DeployBaseConsole.cmd*.

5. Type the tenant ID at the following prompt.

Enter the id of the tenant you want to import the content pack into (Required):

Note: The tenant ID is case-sensitive.

For example, Forward Inc.

The installer automatically detects the existing version of the base model in your environment, the following message appears:

6. Type y to continue to upgrade at the following prompt.

A previous version of CA ASC Foundation is detected, do you want to upgrade to ASC 1.7.1? Press y to upgrade or any key to exit the setup:

Note: If an existing installation is not detected, the installation of CA Automation Suite for Clouds Base Configuration Release 1.7.1 proceeds.

On successful upgrade, BUILD SUCCESSFUL message appears.

If the build has failed, press any key other than 'y' to exit the setup.

7. Press Enter at the following prompt.

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

8. Type y to continue at the following prompt.

Installation will re-start CA Service Catalog multiple times. Please press y to continue or any key to exit: y

9. Press Enter at the following prompt.

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

10. Type the database credentials to configure ASC schema at the following prompts.

Enter Service Catalog Database Administrator (Default sa):

Enter Service Catalog Database Administrator Password:

11. Type y at the following prompt to proceed creating groups.

If build is successful, enter y to Create Groups or any key to exit the setup:

Following groups are created in CA EEM and assigns permissions to the service offerings in CA Service Catalog as defined in the content pack groups properties file:

- ASCgrp_baseconsole_NormalUser
- ASCgrp_baseconsole_Admin

Note: The groups in CA EEM are used for the *Request user to Service group* offering. All the permissions that are assigned in CA Automation Suite for Clouds before upgrade remain unchanged. The CA EEM groups and permissions are in addition to the existing Active Directory groups and set of permissions.

Verify Default Rules

Ensure that the following sets of default CA Service Catalog rules that you disabled during the content deployment are still disabled:

Following rules are located under Request/Subscription item change.

- When Status is Submitted and Approval Process is driven by Workflow.
- When Status is Pending Approval and Requested By and Requested For users are different.
- When Status is Pending Approval.
- When Status is Fulfillment Canceled.
- When Reservation Request is Rejected.
- When Reservation Request is Approved.
- When Status is Pending Fulfillment.

Following rules located under Request Pending action item change.

- When action is Canceled.
- When action is Delegated.
- When action is Returned.
- When action is Taken.
- When action is Transferred
- When Fulfilled.
- When Pending Approval actions are Assigned.
- When Pending Approval actions are Assigned and Requested By and Requested For users are different.
- When Pending Fulfillment actions are Completed.
- When Status is Approved.
- When Status is Rejected.
- When Pending Fulfillment actions are Assigned.

Verify Datasets

After you deploy the upgrade, verify the following dataset in CA Process Automation:

- ASC_Security_GlobalDataset
 - Login Parameters CHANGE ME
 - APP URLs CHANGE ME
 - AD Parameters CHANGE ME
 - EEM Parameters

Verify Upgrade

Verify the upgrade by performing the following steps:

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, and Content Packs.

Content packs installed before and after CA Automation Suite for Clouds upgrade appears.

3. Verify that names and ID after upgrade appears correctly.
4. Verify that all users are available and you are able to log in to CA Service Catalog.
5. Verify that the users created using the User Onboarding procedure are available.

After you complete upgrading the CA Automation Suite for Clouds Foundation, continue upgrading the CA Automation Suite for Clouds Base Configuration for ESX deployed in your environment.

Upgrade CA Automation Suite for Clouds Base Configuration ESX Content

This section details the content upgrade procedures for CA Automation Suite for Clouds Base Configuration for ESX.

Review Prerequisites

Complete and verify the following items before you start upgrading the ESX content pack for CA Automation Suite for Clouds Base Configuration:

- Verify that CA Automation Suite for Clouds Foundation upgrade is complete.
- Make sure that ASC_Security_GlobalDataset is checked in and closed.

To verify, open the CA Process Automation client that is configured with existing CA Automation Suite for Clouds. Navigate to Default Environment: Orchestrator. If ASC_GlobalDataset is checked out and open, check in and close. If the data set is in the checked out state, upgrade can fail to update the data set.

Upgrade Content

Before you start upgrading, rename all the existing folders under the content packs folder with a suffix, _old. This step prevents conflict among the new files that you are going to deploy.

Follow these steps:

1. Unzip *CA ASC Server Automation - ESX.zip* contents from the media to %USM_HOME%/filestore/contentpacks.
2. Open a CA Service Catalog Command Prompt window, change directory to %USM_HOME%/filestore/contentpacks/CA ASC Server Automation - ESX.
3. Run *DeployServerAutomation-ESX.cmd*.
4. Type the tenant ID at the following prompt.

Enter the id of the tenant you want to import the content pack into (Required):

Note: The tenant ID is case-sensitive.

For example, Forward Inc.

The Installer automatically detects the existing version of the content pack in your environment, the following message appears:

5. Type y to continue to upgrade.

An earlier version of CA ASC SA ESX Cartridge is detected, do you want to upgrade to ASC 1.7.1? Press y to upgrade or any key to exit the setup:

If an existing installation is not detected, the installation of CA Automation Suite for Clouds Base Configuration Release 1.7.1 proceeds.

6. Type y at the following prompt to proceed with upgrade.

Installation will re-start CA Service View multiple times. Please press y to continue or any key to exit:

On successful upgrade, the BUILD SUCCESSFUL message appears.

If the build fails, enter any key other than y to exit the setup.

7. Press Enter at the following prompt.

Enter the name of CA PAM configuration to import process definitions to specific CA PAM instance. Leave it blank to import process definitions into the default CA PAM instance [INSTALLED_DEFAULT]

8. Type the database credentials to configure ASC schema at the following prompts.

Enter Service Catalog Database Administrator (Default sa):

Enter Service Catalog Database Administrator Password:

9. Type y at the following prompt to proceed creating groups.

If build is successful, enter y to Create Groups or any key to exit the setup:

After the groups are successfully created, the following message opens.

Offering permissions set successfully in CA Service Catalog.

The following groups are created in CA EEM and assigns permissions to the service offerings in CA Service Catalog as defined in the content pack groups properties file:

- ASCgrp_sa_esx_Snapshots
- ASCgrp_sa_esx_DataStore
- ASCgrp_sa_esx_Reservation_Create
- ASCgrp_sa_esx_Reservation_Extend
- ASCgrp_sa_esx_Reservation_Return
- ASCgrp_sa_esx_Reservation_Change

Note: The newly created groups in CA EEM are used for the *Request user to Service group* offering. All the permissions and groups that are created in CA Automation Suite for Clouds before upgrade remain unchanged. The new groups and permissions are in addition to the existing set of permissions and groups.

Verify Datasets in CA Process Automation

After you deploy the CA Automation Suite for Clouds Base Configuration for ESX upgrade, verify the following datasets in CA Process Automation:

- ASC_GlobalDataset under the CA ASC folder.
 - Login Parameters
 - APP URLs CHANGE ME

Verify Upgrade

Verify the upgrade by performing the following steps:

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, and Content Packs.
Content packs installed before and after CA Automation Suite for Clouds upgrade appears.
3. Verify that names and ID after upgrade appears correctly.

You have completed the CA Automation Suite for Clouds Base Configuration for ESX upgrade. All content packs are upgraded for CA Automation Suite for Clouds Release 1.7.1.

Post Upgrade Configuration

After you upgrade all products, make sure to perform the following configuration to complete the upgrade:

- [Update the vCenter AIM Servers](#) (see page 302) information on CA Server Automation.
- [Configure Super User on CA Server Automation](#) (see page 302).
- [Configure CA Service Catalog](#) (see page 303).
- [Disable Default CA Service Catalog Rules](#) (see page 304).
- After upgrade if the values in the dataset are missing, continue to [configure CA Process Automation Datasets for CA Automation Suite for Clouds Foundation](#) (see page 179).
- After upgrade if the values in the dataset are missing, continue to [configure CA Process Automation Datasets for VMware ESX](#) (see page 199).
- [Configure Touchpoint on CA Server Automation](#) (see page 311).

Update the vCenter AIM Servers

Sometimes after upgrading the CA Server Automation the vCenter AIM Server details disappears. Manually add the missing information to the CA Server Automation configuration.

Follow these steps:

1. Log in to the CA Server Automation server.

Example: <<https://<host name>:<port number>/UI/>>

2. Click Management, Administration, Configuration.
3. From the left menu, click the vCenter Server link from the Provisioning section.
The vCenter Server page opens.
4. Click the + button in the vCenter AIM Server section.
Add vCenter AIM Server dialog pops-up.
5. Complete the following details, and click OK:

vCenter AIM Server

Specifies the vCenter AIM Server name.

vCenter Server

Specifies the vCenter Server name.

6. Verify that a green check mark icon appears in Status.

Configure Super User on CA Server Automation

Perform the following procedure to enable the ability for multiple users to manage the reservations lifecycle.

Follow these steps:

1. Log in to the CA Server Automation server.
2. Open a Command Prompt window, change directory to:
C:\CA\ServerAutomation\bin
3. Run the following command:
`dpmutil -set --super`
4. Type the CA EEM credentials at the prompt.
5. Type 1 at the following prompt:
Enter the number for one of the following, or press enter for default:

6. Type the System Administrator credentials.

On the successful configuration, the Configuration finished successfully message appears. You have completed setting the set super user.

7. Run the following command:

```
dpmutil -get --super
```

8. Type the CA EEM Administrator credentials at the prompt.

The Administrator username and platform details are displayed.

On the successful verification, the Configuration finished successfully message appears again. You have verified the super user configuration.

Configure CA Service Catalog

Perform the following procedure after upgrading CA Service Catalog to Release 12.8.

Follow these steps:

1. Log in to CA Service Catalog as an administrator.
2. Click Administration, Configuration.
3. Click CA Process Automation.
4. Click the Load button.
5. Select the Set imported version of CA Process Automation Objects as current version check box.
6. Select the Make imported Custom Operators/Sensors available check box.
7. Click the Load button.
8. Click OK.
9. Click Configure.
10. Click OK.
11. Log in to the CA Process Automation server as the CA Process Automation Administrator.
12. Click the CA SLCM folder.
13. Double-click SLCM_GlobalDataset, and click Check Out.

14. Click Login Parameters CHANGE ME and enter the following details:

password

Specifies the CA Service Catalog Administrator password.

15. Click Misc Parameters CHANGE ME and complete the following details:

- Update the administrator user ID in the Administrator field, if missing.
- If a Mail Server is configured, enter the Administrator_Email and EmailFromAddress.

16. Click Save, and then Check In the changes.

This procedure enables CA Service Catalog to push the latest CA Process Automation processes into the CA Process Automation server.

Disable Default CA Service Catalog Rules

If you are already using any of the following default CA Service Catalog rules in your environment, we recommend disabling them. Because, default rules create conflict with the CA Automation Suite for Clouds content whenever a request is raised. Additionally, if you have created custom actions for the default CA Service Catalog rules, add the actions again to the new set of rules.

Disable the following rules that are located under Request/Subscription item change:

- When Status is Submitted and Approval Process is driven by Workflow.
- When Status is Pending Approval and Requested By and Requested For users are different.
- When Status is Pending Approval.
- When Status is Fulfillment Canceled.
- When Reservation Request is Rejected.
- When Reservation Request is Approved.
- When Status is Pending Fulfillment.

Disable the following rules that are located under Request Pending action item change.

- When action is Canceled.
- When action is Delegated.
- When action is Returned.
- When action is Taken.
- When action is Transferred.
- When Fulfilled.
- When Pending Approval actions are Assigned.

- When Pending Approval actions are Assigned and Requested By and Requested For users are different.
- When Pending Fulfillment actions are Completed.
- When Status is Approved.
- When Status is Rejected.
- When Pending Fulfillment actions are Assigned.

Configure CA Process Automation Datasets for ESX

Configure the CA Process Automation datasets to provide data to the CA Automation Suite for Clouds Base Configuration automated processes for ESX. For more information about datasets, see the CA Process Automation documentation.

Note: Configure *Error Handling Parameters* in ASC_GlobalDataset and then proceed configuring the datasets that are listed in this topic.

The Datasets capture information of CA Server Automation and Reservation Manager Host, port, userid, and password to connect to CA Server Automation. These details help in provisioning, changing, and snapshot features. In addition, datasets also capture CA Service Catalog, CA Process Automation host, and login credentials to initiate the web services. These details help the solution to get the information from CA Service Catalog and update the request states.

Follow these steps:

1. Log in to the CA Process Automation console.
2. Click the Library tab from the home page.
3. Click the CA ASC folder.
4. Click ASC_GlobalDataset and Check Out.
5. Click Login Parameters CHANGE ME and complete the following details:

userID

Specifies the CA Service Catalog Administrator user name.

Value: spadmin

password

Specifies the CA Service Catalog Administrator password.

businessUnit

Specifies the CA Service Catalog business unit name (This value is case-sensitive).

SAM_User

Specifies the CA Server Automation Administrator user name.

SAM_Password

Specifies the CA Server Automation Administrator password.

SpecAM_Touchpoint

If the CA Process Automation Agent is installed on CA Server Automation, then enter the Touchpoint value. This information is used for the datastore and VMware ESX provisioning.

6. Click APP URLs CHANGE ME and complete the following details:

SLCM_URL

Specifies the CA Service Catalog URL.

ITPAM_URL

Specifies the CA Process Automation URL.

SAM_URL

Specifies the CA Server Automation URL.

7. Click Misc Parameters CHANGE ME and complete the following details:

Administrator_Email

Specifies the administrator email.

VC_ESX_HostName

Specifies the ESX host name. This information is used in VMware ESX provisioning.

VC_Datacenter_Name

Specifies the Datacenter name. This information is used in VMware ESX provisioning.

VC_Server_Name

Specifies the vCenter server name. This information is used in VMware ESX provisioning.

SpecAM_Home

Specifies the CA Server Automation bin folder path. This information is used in VMware ESX provisioning.

SpecAMTouchpoint

Specifies the SpecAM Touchpoint. If the CA Process Automation Agent is installed on the CA Server Automation server, then enter the Touchpoint value. This information is used for the datastore and VMware ESX provisioning.

ESX_HostUser

Specifies the ESX host user name. This information is used in VMware ESX provisioning.

Value: root

ESX_OperationRetry

Specifies the retry count, when the operation fails.

Default: 3

ESX_WaitAttempts

Specifies the number of attempts during the wait period.

Default: 5

ESX_WaitTime

Specifies the time interval between each attempt.

Default: 60

StorageAdminOrAdminGroup

Specifies the storage admin.

WindowsAdmin

Specifies the Windows VM template parameters.

Specify the AdminPassword value for the default template. This value is used when the template is not available in the valuemap. Continue creating index values for each Windows VM Template:

Expand the Windows Admin folder, add Indexed Value. A new parameter set is added.

Expand Parameters, and add the following values:

Template

Specifies the name of the Windows virtual machine template.

AdminUserName

Specifies the user name of the virtual machine that accesses the newly provisioned Windows VM using the template.

Default: administrator

AdminPassword

Specifies the administrator password.

IsPasswordProvided

Specifies whether password is provided or not.

Change the parameter value to True if the password is provided.

Default: False

LinuxAdmin

Specifies the Linux VM template parameters.

Specify the AdminPassword value for the default template. This value is used if the template is not available in the valuemap. Continue creating index values for each Linux VM Template:

Expand the LinuxAdmin folder, Add Indexed Value. A new parameter set is added.

Expand Parameters, and add the following values:

Template

Specifies the name of the Linux virtual machine template.

AdminUserName

Specifies the user name of the virtual machine that accesses the newly provisioned Linux VM using the template.

Default: root

AdminPassword

Specifies the administrator password.

SSHPort

Specifies the port where SSH service is listening on the newly provisioned Linux virtual machine with the template.

Default: 22

UseSudo

Specify true if you want to use the sudo user in the Linux environment. For information about configuring the sudo user, see the [Update the sudoers File](#) (see page 207) section.

IsPasswordProvided

Specifies whether password is provided or not.

Change the parameter value to True if password is provided.

Default: False

PAMHome

Specifies the CA Process Automation installation path.

Example: C:\Program Files (x86)\CA\PAM

StorageOwner

Specifies the name of storage server that is configured with CA Server Automation.

8. Click *AD Login Parameters* CHANGE ME and complete the following details:

Adding these parameters allows you to toad secondary users as local administrator to the provisioned machine.

domainName

name of domain

Example: ca

domainAdmin

Specifies the domain administrator name.

domainAdminPassword

Specifies the domain administrator password.

isDomainAdminPasswordProvided

Specifies whether domain administrator password is provided or not.

Change the parameter value to True if the password is provided.

Default: False

9. Click Pam Parameters CHANGE ME and complete the following details:

pamMachineAdmin

Specifies the CA Process Automation machine administrator user name.

Default: Administrator

pamMachineAdminPassword

Specifies the CA Process Automation machine administrator password.

10. Click Storage and enter the details of the following storage services.

Note: If Storage is configured, highlight the Storage Value Definition for the storage integration.

- storageSpecAMTouchpoint
- storageSpecAM_Host_Admin
- storageSpecAM_Host_Password
- storageTierBronzeLabel
- storageTierSilverLabel
- storageTierGoldLabel

Note: If the CA Process Automation Agent has been installed on CA Server Automation, then enter the Touchpoint in the SpecAM_Touchpoint field.

11. Click Save.
12. Click Check In.
13. Close ASC_GlobalDataset.

You have configured the CA Process Automation content for CA Automation Suite for Clouds Base Configuration for ESX.

Configure Touchpoint in CA Server Automation

Perform the following procedure to configure a touchpoint that is required for creating the datastore. This procedure requires you to first install the CA Process Automation agent on the CA Server Automation server, and then configure the touchpoint.

Follow these steps:

1. Log in to the CA Server Automation server.
2. Open a web browser and launch CA Process Automation client.
3. Log in as CA Process Automation Administrator (pamadmin).
4. Click the Configuration tab.
5. Click the Installation palette.
6. Click Install for Install Agent
7. At the File Download prompt, click Run to start the installer. If you receive a security warning, click Run.

The Language Selection dialog opens. The language of the host computer is selected by default.

8. Click OK or select another language and click OK.

The welcome page of the CA Process Automation Agent Setup wizard appears.

9. Click Next.

The License Agreement opens.

10. Read the license. If you accept the terms, click I accept the terms of the License Agreement. Click Next.

The Set Java Home Directory page opens.

11. If the displayed Java home directory is not correct, browse to the JRE folder.

The default JRE folder for Windows follows, where jre has a release-specific name:

C:\Program Files\Java\jre

12. Click Next.

The Select Destination Directory page opens. The default path follows:

C:\Program Files\CA\PAM Agent

13. Click Next to accept the default or enter a destination directory for the new agent, and click Next.

The Select Start Menu Folder page opens.

14. (Windows only) Click Next to accept CA Process Automation Agent as your Start menu shortcut or type a new name and click Next.

15. (Optional) Create short cuts for all users on this host.

16. (Optional) Suppress the short-cut creation entirely.

17. Examine the Domain URL and the URL of the Domain Orchestrator from which you launched the agent installation. Click Next.

18. Complete the General Properties page as follows:

a. Accept the Agent Host name entry. This name identifies the host from which you started the installation.

b. Change or accept the default Display Name, the host name.

c. Accept 7003 as the Agent Port unless this port is used. Alternatively, enter another port number such as 57003.

d. If you launched the agent installation from a Windows host, select Install as Windows Service.

e. (Optional) Select Start Agent After Installation.

Starting the agent lets you view the active agent and continue with the agent configuration.

19. Click Next to accept the default temporary directory for executing scripts or enter another path and then click Next.

Note: An acceptable path contains no spaces.

The Set PowerShell execution policy page opens.

20. Read the displayed explanation and complete the setting in one of the following ways.

- If you use Windows PowerShell, select the Remote Signed check box to set the PowerShell execution policy and browse to the PowerShell host location. Click Next.

This setting enables you to run Windows PowerShell scripts through this agent.

- If you do not use Windows PowerShell, click Next.

The CA Process Automation agent installation begins.

21. Click Finish.
22. Start the agent service. Click Start, Programs, CA, *agent-name*, Start agent service.
23. Click the Configuration Browser palette on the Configuration tab.
24. Click Refresh.
25. Expand Agents and verify that your agent name is listed.

Continue configuring touchpoint in CA Process Automation.
26. Expand Configuration.
27. Click the Configuration Browser palette.
28. Expand Domain.
29. Right-click Default Environment, and select Lock.
30. Expand Agents, right-click the agent name, select Configure touchpoint at, Default Environment.
- The Add Agent Touchpoint popup appears.
31. Enter the name of the touchpoint and click OK.

The newly added touchpoint appears under All Touchpoints, under Domain, Default Environment.
32. Click Save.
33. Right-click Default Environment, and select Unlock.

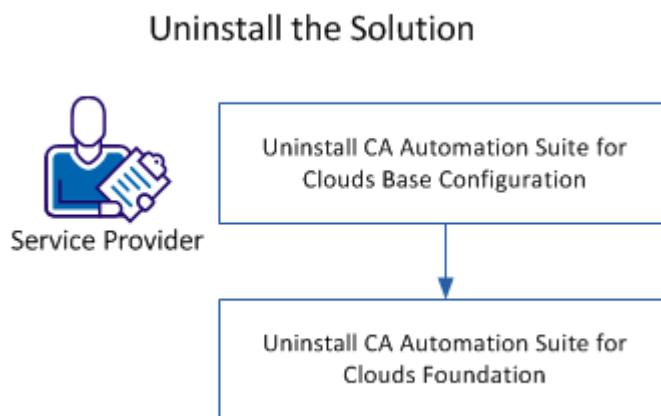
You have configured the touchpoint on the CA Server Automation server.

Chapter 6: Uninstall the Solution

As a Service Provider, you can uninstall CA Automation Suite for Clouds Base Configuration when you no longer need it.

Important! Uninstall CA Automation Suite for Clouds Base Configuration for ESX first and then uninstall the CA Automation Suite for Clouds Foundation.

The following diagram illustrates how a Service Provider uninstalls the solution:



Follow these steps:

1. [Uninstall CA Automation Suite for Clouds Base Configuration for ESX](#) (see page 315).
2. [Uninstall CA Automation Suite for Clouds Foundation](#) (see page 318).

Uninstall CA Automation Suite for Clouds Base Configuration for ESX

Uninstall CA Automation Suite for Clouds Base Configuration by performing the steps that are provided in this section.

Delete Data Views

You delete data views to remove the report builder settings.

Follow these steps:

1. Log in to CA Service Catalog as an Administrator.
2. Click Administration, Report Builder, Data Views.
3. Expand the Chargeback folder from the Data View List.
4. Delete the following data views:
 - Get Server Costs By Cost Center
 - Get VM Reservations By Cost Center
 - Get VM Reservations For Month
 - Get Server Costs By Cost Center - SSRM
 - Get VM Reservations By Cost Center - SSRM
 - Get VM Reservations For Month - SSRM

You have deleted the data views that are associated with chargeback.

Uninstall Content Packs

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, Content Packs.
3. Click the CA ASC Server Automation - ESX content pack.
4. Click Uninstall.

Note: Verify that the *Status* of all the items in the Content section is in Enabled state before you click uninstall.

Note: If you are uninstalling from an upgraded environment, it is important to follow the order to complete the uninstall process. For CA Automation Suite for Clouds Release 1.7.1, uninstall the *CA ASC Server Automation - ESX (CA_ASC_SA_ESX_v1.7.1_en)* content pack.

The selected content pack is uninstalled.

Remove CA Process Automation Content

Follow these steps:

1. Open CA Process Automation client.
2. Click the Library tab and navigate to the Orchestrator.
3. Delete the CA ASC folder.
4. Empty the Recycle Bin to permanently delete files.

Remove plugin.jar Files from CA Service Catalog

Follow these steps:

1. Log in to the CA Service Catalog server.
2. Stop CA Service Catalog service from the Windows Services console.
Note: For CA Service Catalog 12.8, stop the CA Service Catalog service.
3. Browse to the %USM_HOME%\view\webapps\usm\WEB-INF\lib folder.
Note: For CA Service Catalog 12.8, browse to the %USM_HOME%\lib folder.
4. Locate the following jar file and delete the file.
`ASCESXPlugins.jar`
5. Navigate to %USM_HOME%\filestore\plugins/ and delete the following folders:
 - com.ca.asc.sa.esx.chargeback.plugins.org-plugin
 - com.ca.asc.sa.esx.chargeback.plugins.template-plugin
 - com.ca.asc.sa.esx.chargeback.plugins.eemgroups-plugin
 - com.ca.asc.sa.esx.chargeback.plugins.servicefolder-plugin
 - com.ca.asc.sa.esx.chargeback.plugins.costcenter-plugin
 - com.ca.asc.sa.esx.chargeback.plugins.department-plugin
 - com.ca.asc.sa.esx.chargeback.user-reservations-select-plugin
6. Start the CA Service Catalog service from the Windows Services console.
Note: For CA Service Catalog 12.8, start the CA Service Catalog service.

Remove CA EEM groups from CA EEM

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Administration, Users.

3. Click the CA-EEM button.
The CA EEM screen opens.
4. Select the CA Service Catalog instance from the Application drop-down, and log in to CA EEM.
5. Navigate to the Manage Identities tab, select Groups submenu.
6. Click the Go button to list all groups.
7. Select the following groups one after the other, and click the Delete icon to remove the CA EEM group:
 - ASCgrp_sa_esx_Snapshots
 - ASCgrp_sa_esx_DataStore
 - ASCgrp_sa_esx_Reservation_Create
 - ASCgrp_sa_esx_Reservation_Extend
 - ASCgrp_sa_esx_Reservation_Return
 - ASCgrp_sa_esx_Reservation_Change
 - ASCgrp_sa_esx_Power_Functions
 - ASCgrp_sa_esx_offering_admin

Remove Storage Tables from Database

Follow these steps:

1. Log in to the database (MDB) using sa credentials.
2. Delete the following tables in the same order as listed:
 - a. usm_asc_department
 - b. usm_asc_cost_center
 - c. usm_asc_policy_org
 - d. usm_asc_policy_master
 - e. usm_asc_policy_price
 - f. usm_asc_storage

Uninstall CA Automation Suite for Clouds Foundation

After you uninstall CA Automation Suite for Clouds Base Configuration, follow the steps that are provided in this section to uninstall CA Automation Suite for Clouds Foundation.

Uninstall Content Pack

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Catalog, Configuration, Content Packs.
3. Click the CA ASC Foundation content pack.

Note: Verify that the *Status* of all the items in the Content section is in Enabled state before you click uninstall.

4. Click Uninstall.

Note: If you are uninstalling from an upgraded environment, it is important to follow the order to complete the uninstall process. For CA Automation Suite for Clouds Release 1.7.1, uninstall the *ASC Foundation Console (CA_ASC_FC_v1.7.1_en)* content pack.

The selected content pack is uninstalled.

Remove CA Process Automation Content

Follow these steps:

1. Open the CA Process Automation client.
2. Click the Library tab, and navigate to the Orchestrator.
3. Delete the *CA ASC Base Console* folder.
4. Empty the Recycle Bin to permanently delete files.

Enable CA Service Catalog Default Rules

Follow these steps:

1. Log in to CA Service Catalog.
2. Navigate to the Administration tab.
3. Select Event-Rules-Actions.
4. Select Request Subscription Item Change.

5. Enable the following rules:
 - When Reservation Request is Approved
 - When Reservation Request is Rejected
 - When Status is Fulfillment Canceled
 - When Status is Pending Approval
 - When Status is Pending Fulfillment
 - When Status is Pending Approval and Requested By and Requested For users are different
 - When Status is Submitted and Approval Process is driven by Workflow
6. Click Done.
7. Select Request Pending Action Change.
8. Enable the following rules:
 - When action is Canceled
 - When action is Delegated
 - When action is Returned
 - When action is Taken
 - When action is Transferred
 - When Fulfilled
 - When Pending Approval actions are Assigned
 - When Pending Approval actions are Assigned and Requested By and Requested For users are different
 - When Pending Fulfillment actions are Assigned
 - When Pending Fulfillment actions are Completed
 - When Status is Approved
 - When Status is Rejected
9. Click Done.

Remove plugin.jar Files from CA Service Catalog

Follow these steps:

1. Log in to the CA Service Catalog server.
2. Stop CA Service Catalog service from the Windows Services console.

Note: For CA Service Catalog 12.8, stop the CA Service Catalog service.

3. Browse to the %USM_HOME%\view\webapps\usm\WEB-INF\lib folder.
Note: For CA Service Catalog 12.8, browse to the %USM_HOME%/lib folder.
4. Locate the following JAR file and delete the file.
FoundationConsolePlugins.jar
5. Navigate to %USM_HOME%/filestore/plugins/ and delete the *com.ca.puma.base.console.plugins-get-user-groups* folder.
6. Start the CA Service Catalog service from the Windows Services console.
Note: For CA Service Catalog 12.8, start the CA Service Catalog service.

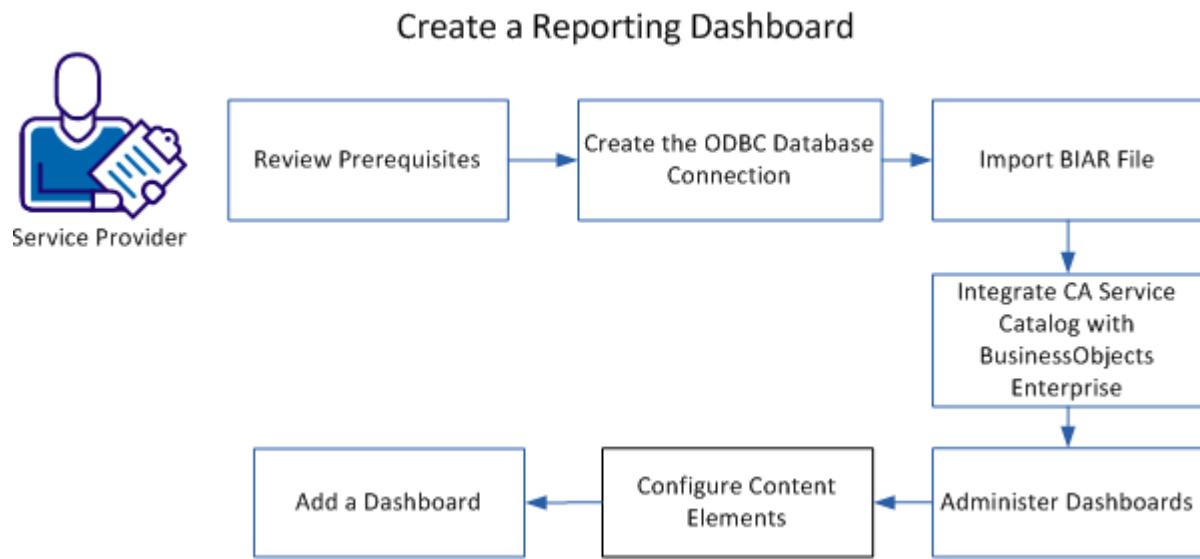
Remove CA EEM groups from CA EEM

Follow these steps:

1. Log in to CA Service Catalog.
2. Navigate to Administration, Users submenu.
3. Click the CA-EEM button.
The CA Embedded Entitlements Manager screen opens.
4. Select the CA Service Catalog instance from the Application drop-down, and log in to CA EEM.
5. Navigate to the Manage Identities tab, select Groups submenu.
6. Click the Go button to list all groups.
7. Select the following groups one after the other, and click the Delete icon to remove the CA EEM group:
 - ASCgrp_baseconsole_NormalUser
 - ASCgrp_baseconsole_Admin

Chapter 7: Create a Reporting Dashboard

As a Service Provider you create and configure the CA Business Intelligence (BusinessObjects XI) reporting server for the Service Delivery Manager (or their delegates) who generates reports.



Follow these steps:

1. [Review the Prerequisites](#) (see page 324).
2. [Create the ODBC Database Connection](#) (see page 324).
3. [Import the BIAR file](#) (see page 327).
4. [Integrate CA Service Catalog with BusinessObjects Enterprise](#) (see page 328)
5. [Administer Dashboards](#) (see page 331).
6. [Configure Content Elements](#) (see page 332).
7. [Add Dashboards](#) (see page 334).

Review the Prerequisites

To complete all tasks in the scenario, you must have the following items:

- Access to the CA Business Intelligence server and the following parameter values:
 - BoHost (Name of the CA Business Intelligence server)
 - BoUser (CA Business Intelligence Username, typically Administrator)
 - BoPassword (CA Business Intelligence password)

These values are required for you to complete the import BIAR file.

- Access to the CA Business Intelligence Enterprise Java InfoView server
- Access to the BusinessObjects Enterprise server.
- Access to the CA Server Automation server.
- Access to the BIAR file and CA Server Automation installation media.

Note: You can find the required information in the [installation worksheet](#) (see page 19).

Create the ODBC Database Connection

You can create an ODBC database connection on both CA Server Automation server and CA Business Intelligence server.

Create DSN on the CA Server Automation Server

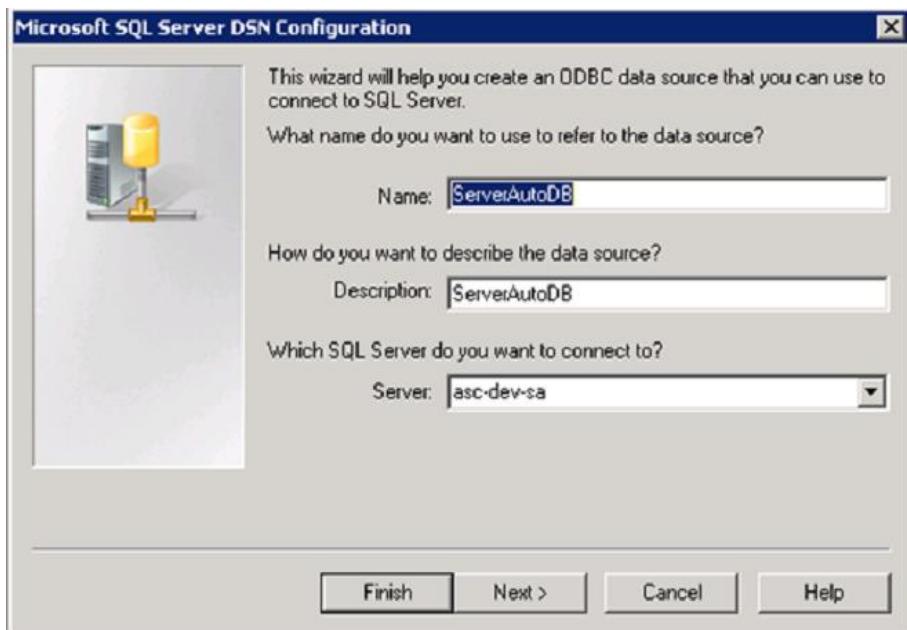
Create a system Data Source Name (DSN) to the underlying CA Server Automation database (SQL database) before using the CA Server Automation reports in CA Business Intelligence.

Follow these steps:

1. Click Start, Administrative Tools, Data Sources (ODBC) on the CA Server Automation server.
The ODBC Data Source Administrator window appears.
2. Click the System DSN tab, and click Add.

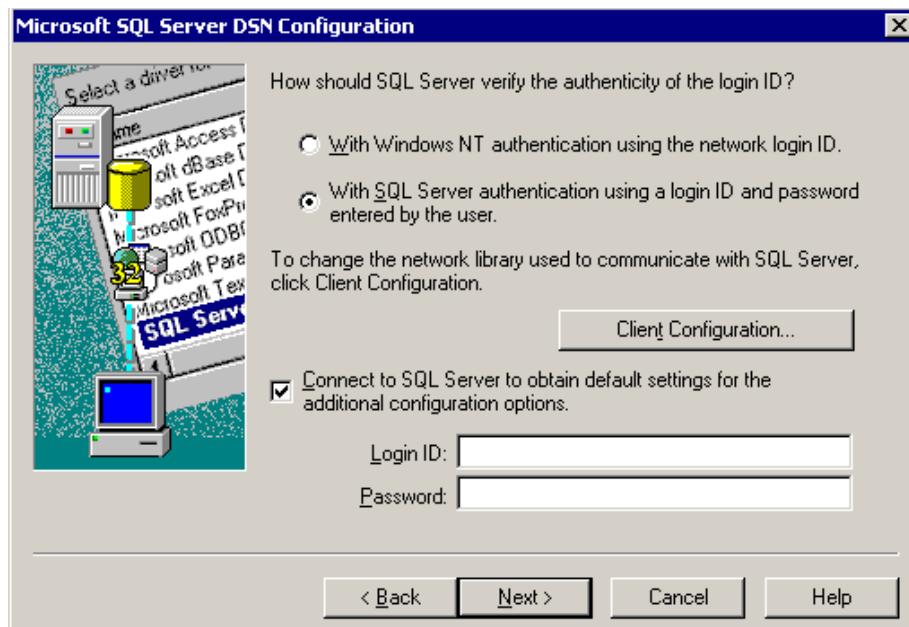
3. Select the SQL Server driver for your data source and click Finish.

The wizard opens for you to create a data source and connect to SQL Server.



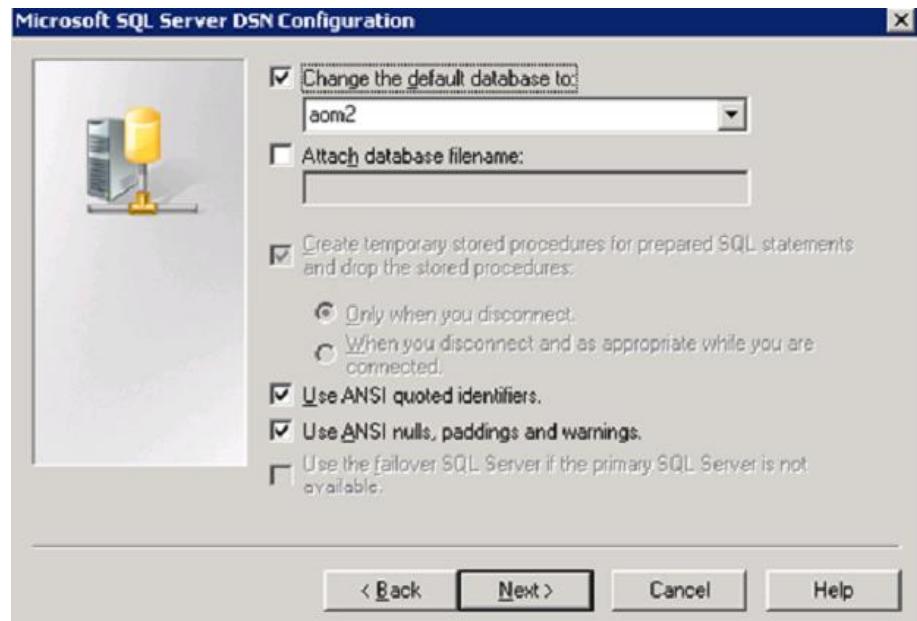
4. Complete the following details, and click Next:

The authentication page opens.



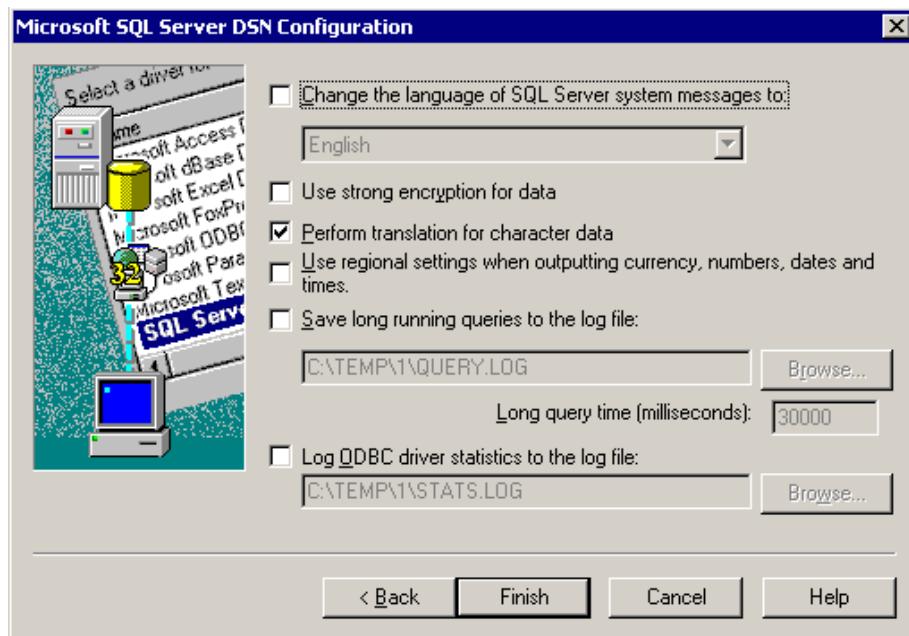
5. Select the following options and click Next:
 - a. Select the **With SQL Server authentication using a login ID and password entered by the user** option.
 - b. Select the **Connect to SQL Server to obtain default settings for the additional configuration options** check box.
 - c. Type the SQL Server Database Login ID and Password, and click Next.

The default database page opens.



6. Select the database name from the drop-down list, and click Next.

The default configuration page opens.



7. Use the default configuration, and click Finish.
8. Test the Data Source connection.
9. Click OK.
10. Click OK to complete DSN creation for CA Business Intelligence.

The DSN is created.

Create DSN on CA Business Intelligence Server

Perform the same steps as detailed in Create DSN on the CA Server Automation Server section for the CA Business Intelligence server.

Import the BIAR file

You import the BIAR file to view CA Business Intelligence reports for CA Server Automation. The BIAR file consists of CA Server Automation reports and universes. All users must import the BIAR file manually to view reports in the Enterprise Java InfoView application.

Follow these steps:

1. Access the CA Automation Suite for Clouds media.
2. Copy the contents of the DVD1\Reports directory into the installed destination folder on the CA Server Automation server.
For example: C:\Program Files\CA\Server Automation\Reports.
3. Apply read/write permissions to the Reports\BIConfig directory.
4. Modify the *am_biar_import.xml* file and replace the required properties.

This file contains information for the BIAR file name and DB credentials.

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <!-- Import BIAR file -->
  <step priority="1">
    <add>
      <biar-file name="C:\ServerAutoReports\Reports\ServerAutomation.biar">
        <networklayer>ODBC</networklayer>
        <rdms>MS SQL Server 2005</rdms>
        <username>sa</username>
        <password>*****</password>
        <datasource>ServerAutoDB</datasource>
        <server>asc-dev-sa</server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

Important! For security reasons, clear the DB credentials from the xml import file after the BIAR file is imported.

5. Modify the *importCABIReports.bat* file and set the CA_DPM_HOME environment variable:

```
SET CA_DPM_HOME=C:\Program Files\CA\Server Automation
```

6. Run the *importCABIReports.bat* utility.

The BIAR file is imported.

Verify the BIAR File Import

Log in to the Enterprise Java InfoView and verify that the folder by name CA Server Automation Reports is created and associated reports are available.

Integrate CA Service Catalog with BusinessObjects Enterprise

Specifying the configuration settings for BusinessObjects Enterprise is a required task for enabling the integration between BusinessObjects Enterprise and CA Service Catalog. If you are running multiple instances of BusinessObjects Enterprise, these settings apply to all instances.

Set and Test Administration Configuration Parameters

Follow these steps:

1. Log in to CA Service Catalog.
2. On the Administration tab of CA Service Catalog, click Configuration and scroll to the CA Business Intelligence section.
The CA Business Intelligence configuration options appear.
3. Click the Modify (Pencil) icon to next to each property that you want to update, using the following information:

Enable HTTPS

Specifies a web protocol, as follows:

- Select No (the default) to use HTTP to communicate with BusinessObjects Enterprise.
- Select Yes to use HTTPS to communicate with the BusinessObjects Enterprise.

Important! If you select Yes, verify that BusinessObjects Enterprise is using HTTPS. If necessary, configure it to use HTTPS; for details, see the BusinessObjects Enterprise documentation.

Host Name

Specifies the computer name on which the InfoView component of BusinessObjects Enterprise is hosted.

Port Number

Specifies the port number on which InfoView is running.

Default:8080

4. Click the Launch button and verify the connection between CA Service Catalog and InfoView.

The connection is tested, using the new values that you specified. If the connection fails, try using a different value.

5. Recycle Service View.

The BusinessObjects Enterprise configuration details are updated with the values that you specified.

Configure Trusted Authentication

For best results, we recommend configuring CA Service Catalog and BusinessObjects Enterprise to use a trusted authentication for the integration between the two products. A trusted authentication provides Single Sign-on (SSO). SSO allows CA Service Catalog users to access the InfoView application of BusinessObjects Enterprise directly from the CA Service Catalog UI without logging in to BusinessObjects Enterprise.

Follow these steps:

1. Log in to the BusinessObjects Enterprise Central Management Console as a user with administrative rights.
2. Go to the Authentication Management area of the Central Management Console.
3. Click the Enterprise tab.
4. Enable trusted authentication.
5. Enter a shared secret password for your users.

Note: Verify that the value of the password and the frequency that you update meet the password security standards of your organization.

The BusinessObjects Enterprise client and the Central Management Console use the shared secret password to create a trusted authentication password.

6. Perform the remaining steps on every Service View computer.
7. Open the file named %USM_HOME%\reporting\CABI\TrustedPrincipal.conf in a text editor.
%USM_HOME% is the location where Service View is installed.
8. Scroll to the following line:
`SharedSecret=password`
For the password, specify the same shared secret password that you entered on the BusinessObjects Enterprise Central Management Console earlier in this procedure.
9. Save the TrustedPrincipal.conf file.
10. Restart the Service View computer.

Important! When you update the password on the BusinessObjects Enterprise Central Management Console, update the same password in the *TrustedPrincipal.conf* file on every Service View computer.

Run Predefined Reports

To see the various types of CA Server Automation data that you can access quickly and easily with BusinessObjects Enterprise reporting, run the predefined reports. The Infoview button appears on CA Service Catalog pages so that you can start BusinessObjects Enterprise from within CA Service Catalog and can run predefined reports quickly.

Follow these steps:

1. In CA Service Catalog, click Home, Reports, InfoView to start BusinessObjects Enterprise.
The BusinessObjects Enterprise home page opens.
2. In BusinessObjects Enterprise, click Home, Document List, Public Folders, CA Server Automation Reports, Reservation Manager Reports.
3. Select from History, Inventory, or Reservation reports.
4. Double-click the report that you want to run.
5. When prompted, specify the parameters for your report.
6. Click Run Query.

You can view the report.

Administer Dashboards

You can create and maintain dashboards to meet the needs of your organization. A dashboard is a personal page containing elements from the dashboard library.

You use the Dashboard Builder to manage the dashboard library. The dashboard library contains content that you can include in dashboards as dash items. To manage the dashboard library, use the Administration, Dashboard Builder menu.

Administrators and other users select the Administration, Dashboard menu to display, and manage dashboards, to extend permissions for their roles.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Administration, Dashboard Builder.
The Dashboard Library folders appear. Displays the dashboards that you have the permission to access.
3. Expand the library tree and find the category for which you want to administer dashboards.

4. (Optional) Install ActiveX components, if prompted.
Note: Some dashboard items require ActiveX. When you first access a Dashboard Builder item, it prompts you to install ActiveX components in your browser. In such cases, follow the prompts to install the ActiveX components. When completed, resume administering the dashboard.
5. Select the option that you want from the Action drop-down list and click Go.
Note: The options vary according to the category that you have selected in the library tree.
6. Repeat these steps as needed for each dashboard that you must administer.
You have added dashboards to administer.

Configure Content Elements

You can configure content elements in dashboards to customize them to meet the needs of your organization.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Administration, Dashboard Builder.
The Dashboard Library folders appear. They display the dashboards that you have the permission to access.
3. Expand the library folder and subfolders.
The details of the selected content element appear in the Content Preview and Content Properties panes.
4. Select the folder where you want to publish the content.
5. Select Publish Content from the Action drop-down and click Go.
The Add New Content window appears.
6. Provide a name for the content and complete the following details:

Content Type

Select External Web Content as the type of content element that configures the content element as a web page URL.

For more information, see [Sample URLs](#) (see page 333).

ACL Settings

Specifies the access control list (ACL) settings.

To specify the level of access for each role to the content element, use these settings.

7. On the Content Properties pane, click Save.

You have configured the content elements.

Sample URLs

CA Automation Suite for Clouds packages boxireporting.jsp which uses OpenDocument to generate URLs for Crystal reports and Web Intelligence documents. OpenDocument is one of many deployed web applications within a BusinessObjects Enterprise system. This third-party component processes incoming URL requests for documents and delivers the correct document to the end user in the appropriate viewer. You can link to many viewable object types with the OpenDocument syntax. The file type of the target document is expected to be a web intelligence document (*wid). The target document will be refreshed when it is rendered. This behavior has been leveraged from the OpenDoc parameters sType and sRefresh.

Examples on Nonparameterized Reports

Sample URL 1:

`http://Service_Catalog_hostname:service_catalog_port/usm/asc/boxireporting.jsp?report=Image Inventory`

Sample URL 2:

`http://Service_Catalog_host:service_catalog_port/usm/asc/boxireporting.jsp?report=Active Reserved Systems`

CA Service Catalog hostname

Host name of the CA Service Catalog server.

CA Service Catalog_port

Port number of the CA Service Catalog server.

report

The name of the document without extension.

Example on Parameterized Reports

`http://Service_Catalog_host:service_catalog_port/usm/asc/boxireporting.jsp?report=Reservations by Organizational Unit&lsS1. Enter Start Time:=07/04/2012&lsS2. Enter End Time:=07/31/2012&lsS3. Select Organizational Unit:=ESX`

lsS[NAME]

Specifies a value for a single prompt. [NAME] is the text of the prompt.

To specify multiple values for a parameter, use lsM[NAME] separated with a semicolon for Webi.

Sample URL:

```
http://Service_Catalog_host:service_catalog_port/usm/asc/boxireporting.jsp?report=Reservations by Organizational Unit&lsS1. Enter Start Time:=07/04/2012&lsS2. Enter End Time:=07/31/2012&lsM3. Select Organizational Unit:=ESX;Hyper-V
```

lsR[NAME]

Specifies a range of values for a prompt. [NAME] is the text of the prompt. Separate the range of values for the prompt by a double period (..)

If the target is a crystal report, the range must be enclosed in square brackets or parentheses. To include a value in the range, use a square bracket next to a value. Use parentheses to exclude.

Sample URL:

```
http://Service_Catalog_host:service_catalog_port/usm/asc/boxireporting.jsp?report=reportname&lsRparamStringDR=h..i
```

Add Dashboards

You add personal or shared dashboards to provide expedited access to information and to frequently used features and functions of CA Service Catalog.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Home, Dashboards.
3. Click the << icon at the top right part of the page, and click Add Dashboard.

The Dashboard Options page appears.

4. Name the dashboard and configure the other options, as follows. Click the Help (question mark) icon for assistance.

The following fields require explanation:

Shared Dashboard

Creates a shared dashboard.

Administrators use shared dashboards to publish information to users. If this option does not appear or you do not select this option, this dashboard is available to you only (personal).

Note: You can create a personal dashboard and can share it later.

When you select Shared Dashboard, several other fields appear. These fields are mutually exclusive. Select one of the following options:

- Accessible by Sub Business Units – Shares this dashboard with users in your business unit and its child business units.
- Accessible by Role – Shares this dashboard with users who have the roles you specify. Specify your own role to the dashboard for your access after it is created.

5. Click Add to create the dashboard.

The new dashboard appears in the dashboard menu and is selected. The rest of the window is blank, because a new dashboard has no dash items.

6. Do the following steps and add dash items:

- a. Click Show Library from the Dashboard Administration menu.

The Dashboard Library appears.

- b. Navigate the Library tree and locate the elements that you want to use on the dashboard.
 - c. Drag the content elements to the place where you want them on the dashboard.

The elements become the dash items. Adjust the size of the dash items as needed.

7. Set the properties of the dash items by clicking the Edit (pencil) icon on the dash item heading.

Note: To delete a dash item from the dashboard, click the Delete (X) icon on the dash item heading.

8. Click Save Layout.

The Catalog system saves the dashboard layout.

You have added the new dashboard and enabled the Service Delivery Manager to generate or view reports.

Chapter 8: Troubleshooting

This chapter contains troubleshooting topics that are related to CA Automation Suite for Clouds Base Configuration.

Software Package Added in CA IT Client Manager is Not Updated in CA Server Automation

Symptom:

When you add a software package to the CA IT Client Manager, CA Server Automation is not updated in a timely manner.

Solution:

Configure the sync interval value when you update the CA IT Client Manager packages.

Follow these steps:

1. Log in to the CA Server Automation server.
2. Navigate to the C:\CA\ServerAutomation\2.8.2.conf folder.
3. Edit the casdaconf.cfg file.
4. Search for the following property name and update the value for your environment:

“CONFIG_KEY_SDA_PACKAGELIST_SYNC_INTERVAL”

The default interval is set to 12 hours.

Event Receiver is not Triggered

Symptom:

Once the virtual machine is provisioned or failed, CA Server Automation triggers an event receiver to the configured CA Process Automation. However if the import rules and actions fail during the CA Automation Suite for Clouds content installation, the event receiver is not triggered.

Solution:

In such cases, import actions and rules manually using the following procedure.

Follow these steps:

1. Log in to the CA Server Automation server.
2. Copy the following files from the downloaded content pack in the util\ServerAuto-Rules folder to the C: drive.
 - ASC_Actions.txt
 - ASC_Rules.txt
3. Follow the procedure in the ReamMe.txt file in the util\ServerAuto-Rules folder.

Example of File Path: C:\Program Files (x86)\CA\Service Catalog\filestore\contentpacks\CA ASC Server Automation - ESX\util\ServerAuto-Rules

The required actions and rules start importing and a confirmation message appears when the rules are imported.

CA Business Intelligence Server Not Found or Down

Symptom:

When logging into the SAP Central Management Console used for managing security in UMS, I received the following error:

Server not found or server may be down (FWM 01003) null.

Solution:

Recycle the SQL Server Agent service and the Server Intelligence Agent service.

Follow these steps:

1. Click Start, Run, Type "services.msc".
2. Restart SQL Server Agent.
3. Click Start, Run, Type Central Configuration Manager.
4. Restart Server Intelligence Agent.

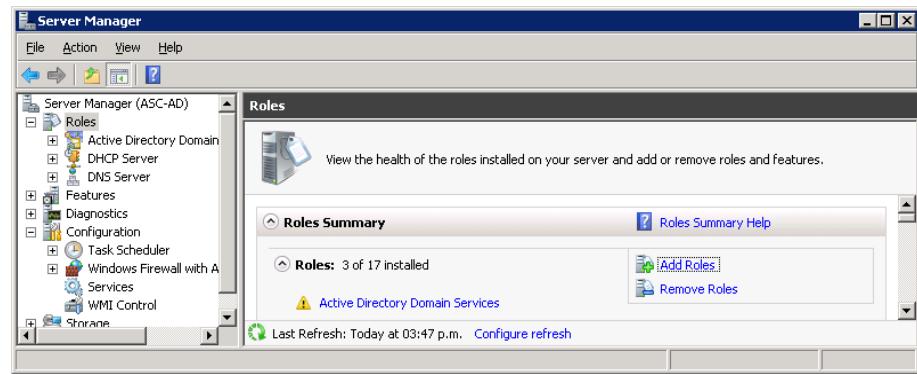
The services are restarted and the server will be available for use.

Appendix A: Active Directory Configuration

How to Add the Active Directory Certification Role to Active Directory

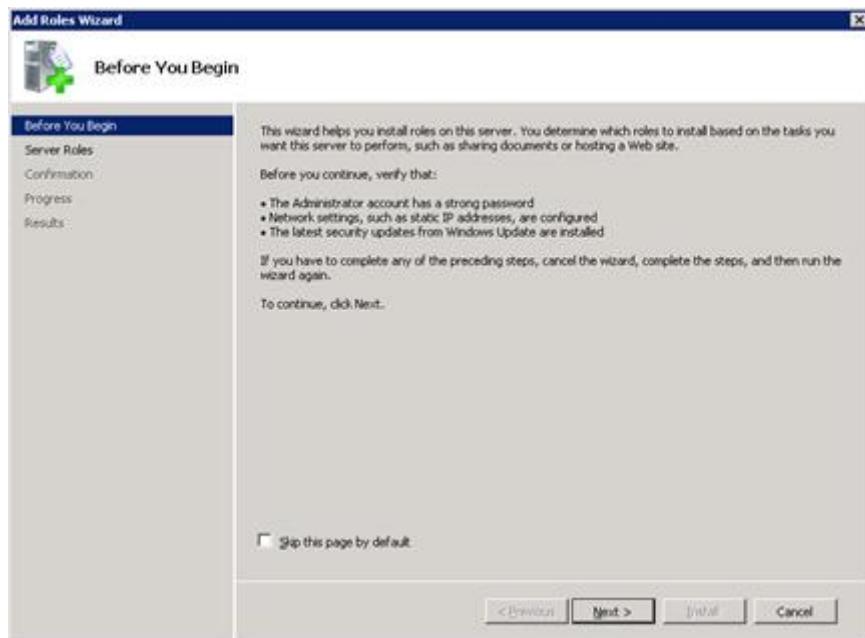
Follow these steps:

1. Log in to the Active Directory Domain Controller as the Domain Administrator
2. Open the Server Manager.



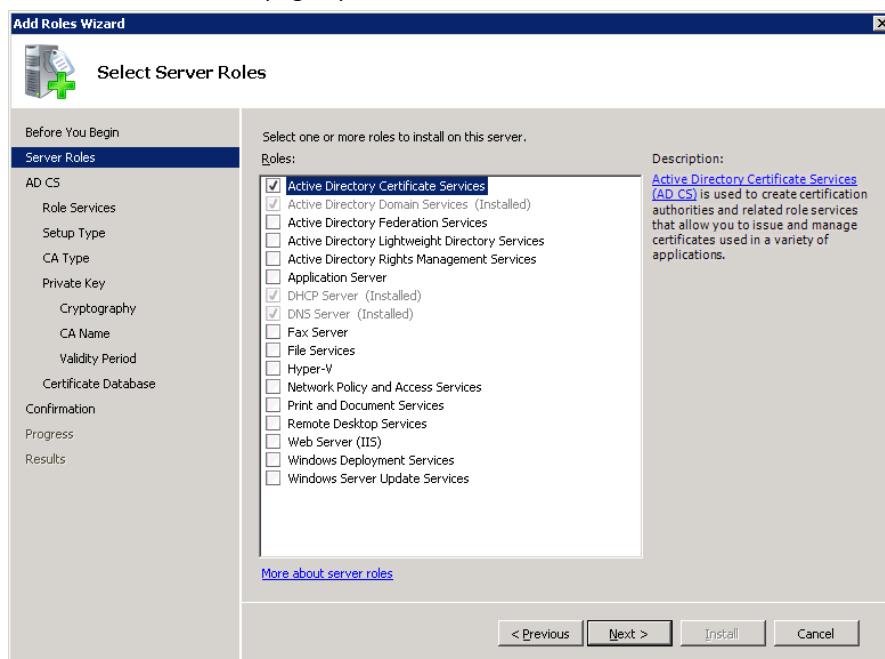
3. Right-click the Computer icon and select Manage.
4. Expand Server Manager, select Roles, and click Add Roles.

The Add Roles page opens.



5. Click Next.

The Select Server Roles page opens.

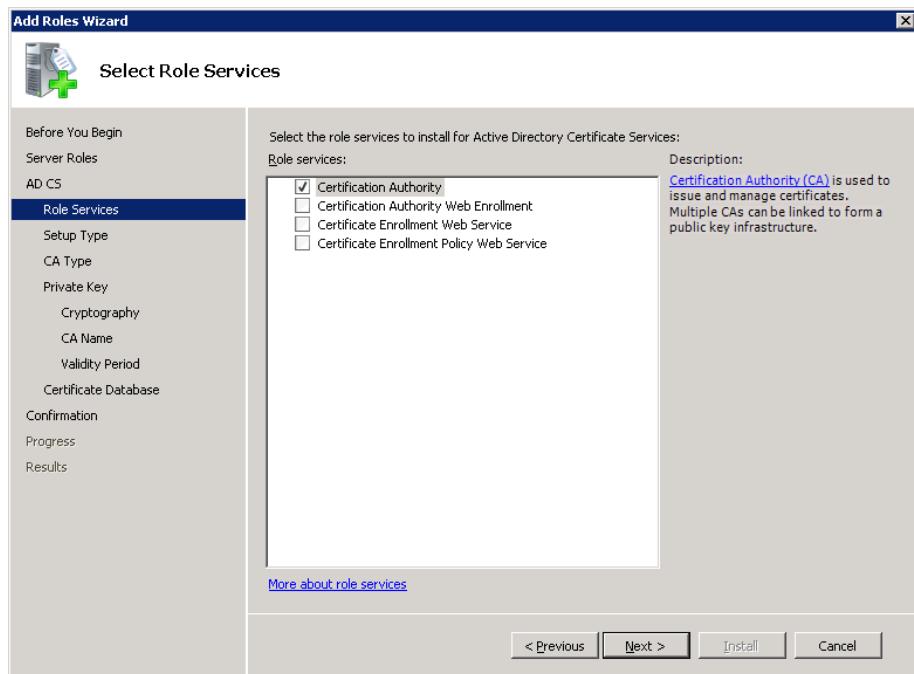


6. Select Active Directory Certificate Services, and click Next.

The Introduction to Active Directory Certificate Services page opens informing you about the services.

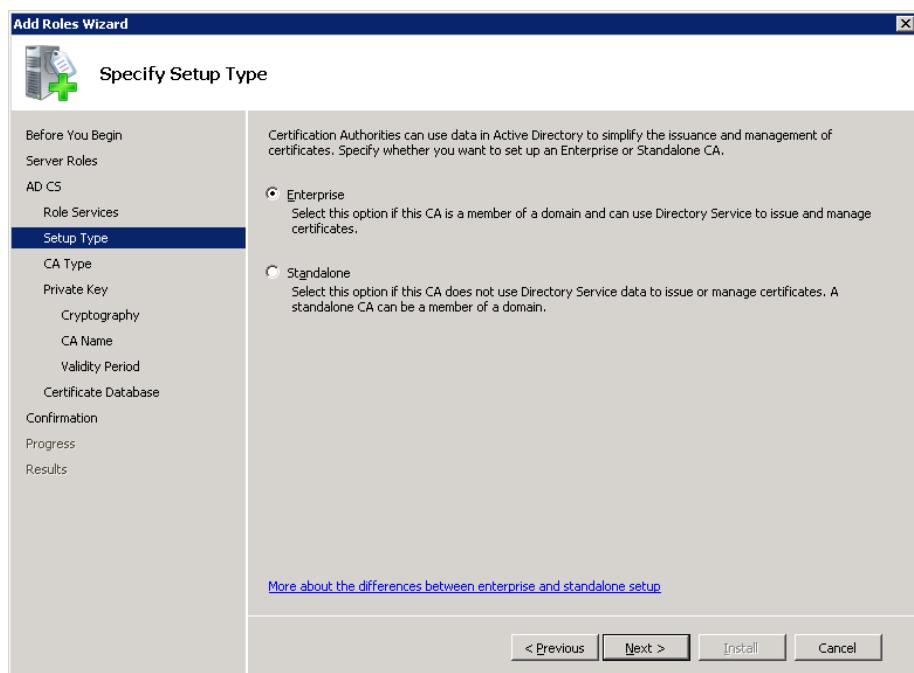
7. Click Next.

The Select Role Services page opens.



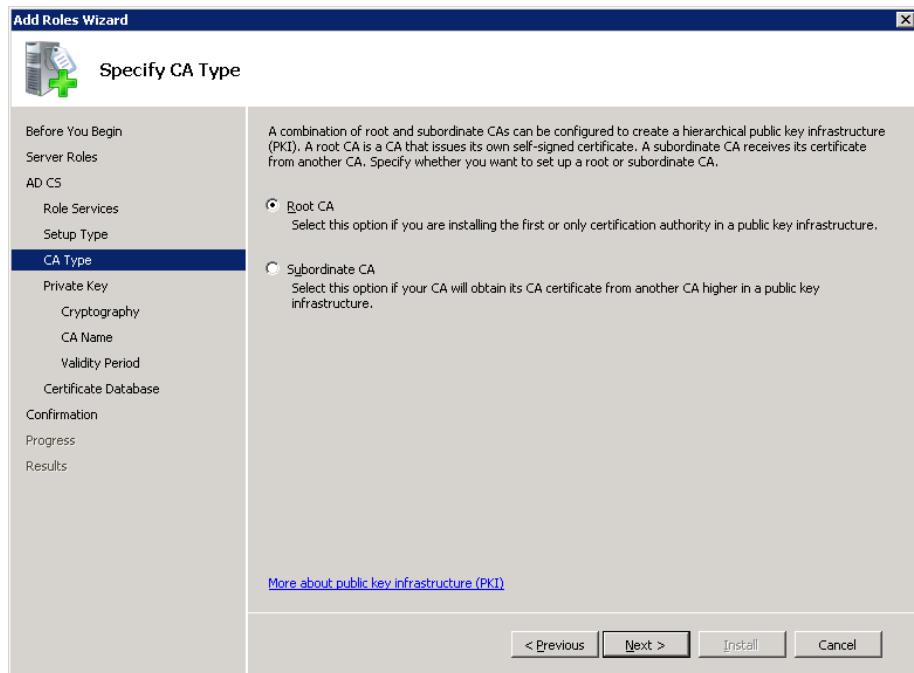
8. Select Certification Authority, and click Next.

The Specify Setup Type page opens.



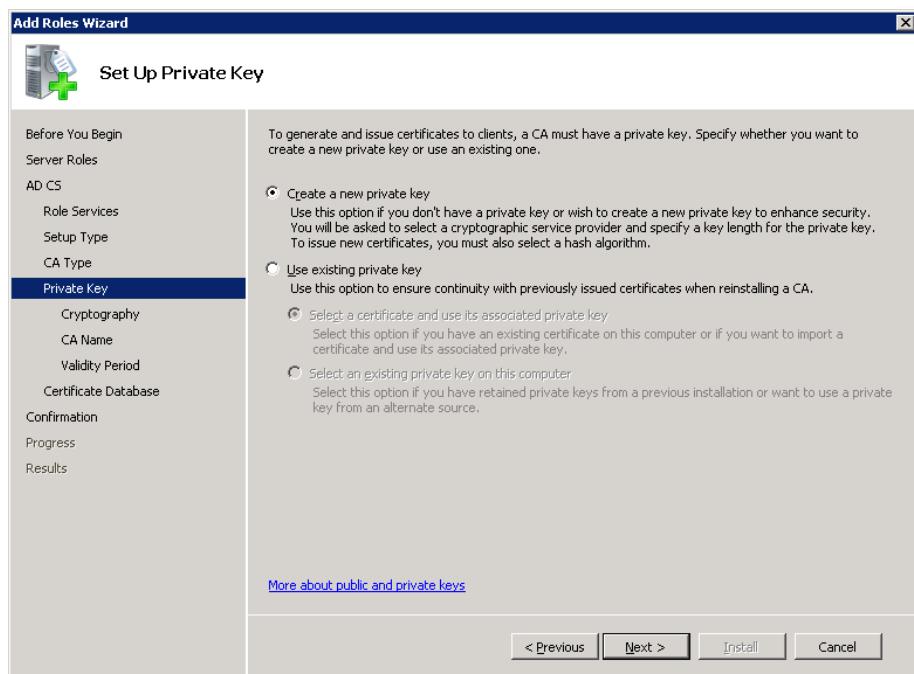
9. Select Enterprise, and click Next.

The Specify CA Type page opens.

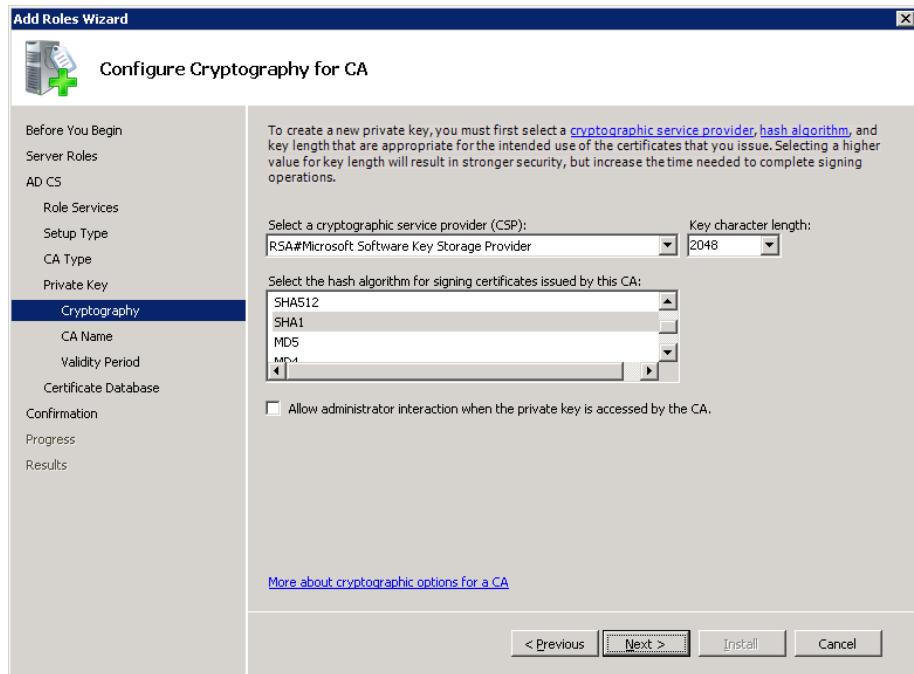


10. Select Root CA, and click Next.

The Set Up Private Key page opens.



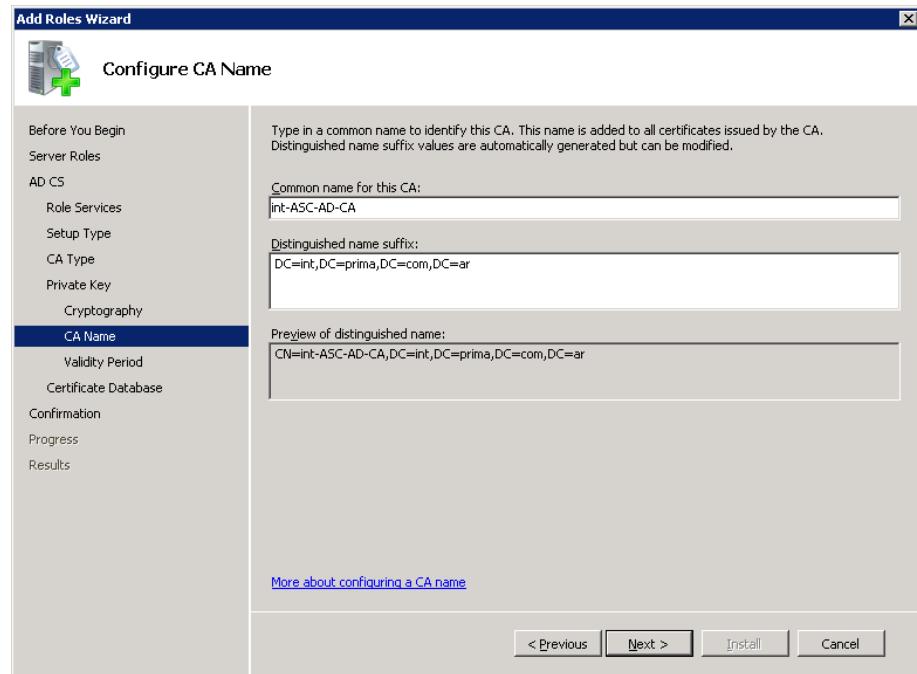
11. Select Create a new private key, and click Next.



12. Complete the following fields:

- Select RSA#Microsoft Software Key Storage Provider from the CSP drop-down list.
- Select 2048 from the Key character length drop-down list.
- Select SHA1 as the hash algorithm for signing certificates.
- Ensure the check box Allow administrator interaction when the private key is accessed by the CA is clear.
- Click Next.

The Configure CA Name page opens.

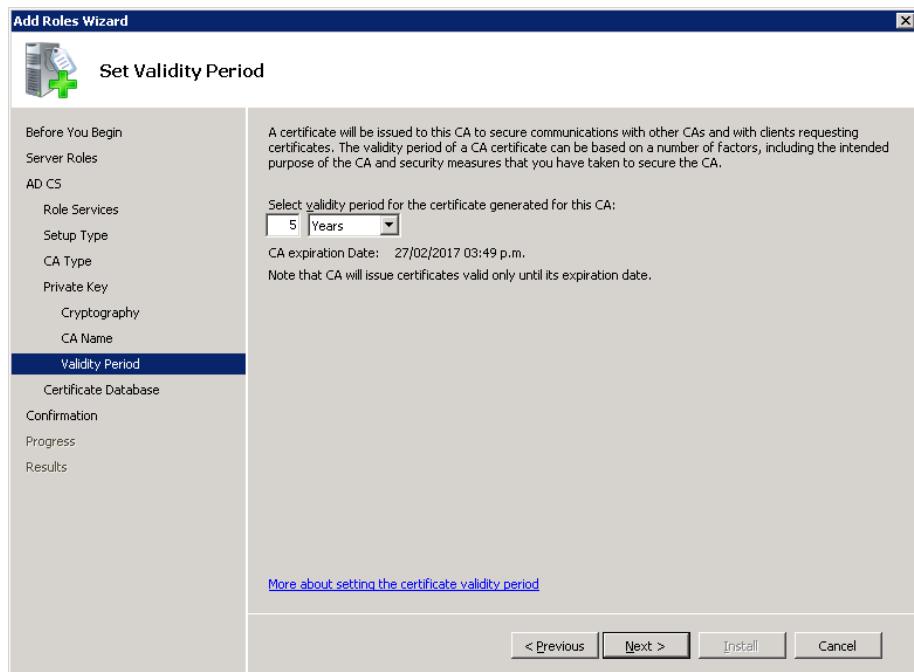


13. Complete the following fields:

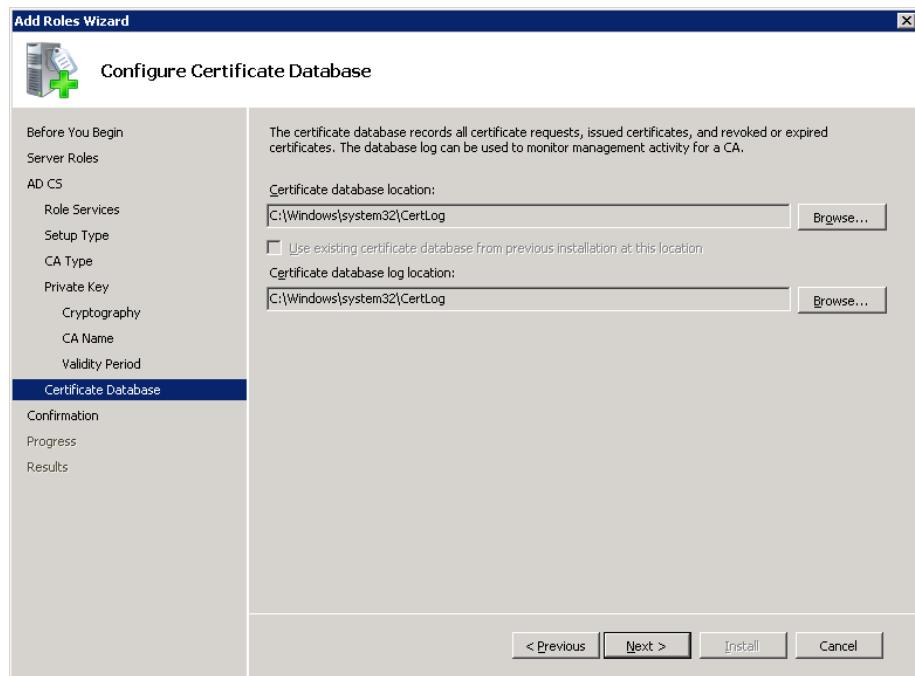
- Enter a name in the Common name for this CA field.
- Enter a suffix to the name in the Distinguished name suffix field.
- Preview the name in the Preview of distinguished name field.

14. Click Next.

The Set Validity Period page opens.



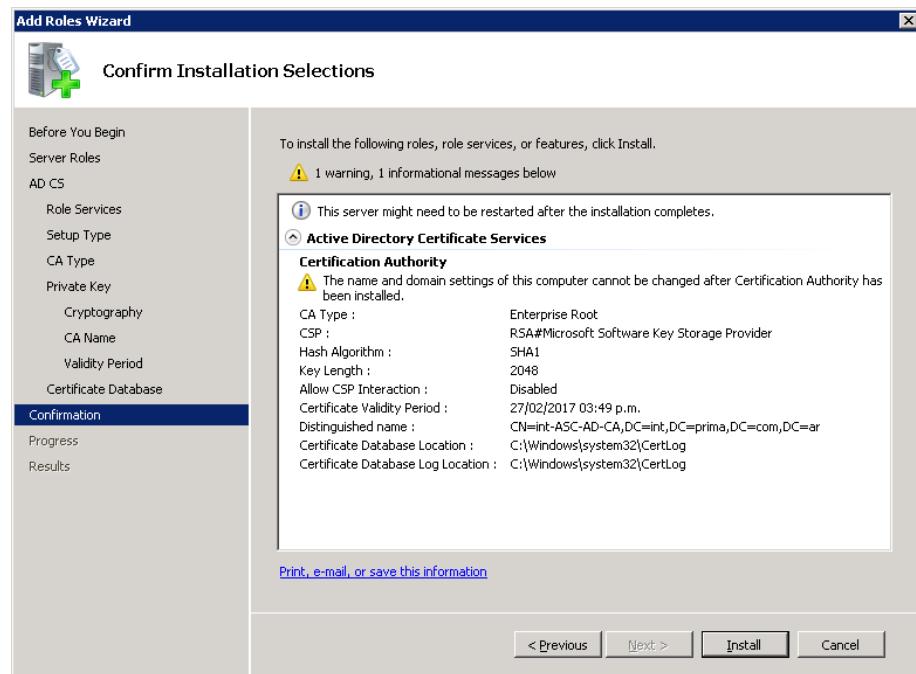
15. Set the validity period, and click Next.



16. Complete the following fields:

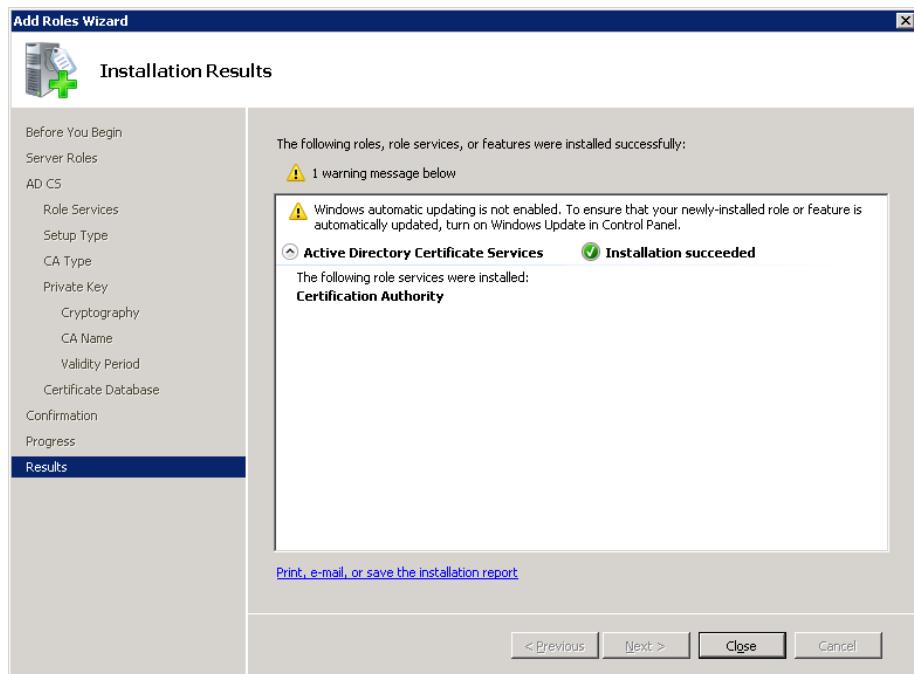
- Verify or change the Certificate database location.
- Verify or change the Certificate database log location.
- Click Next.

The Confirm Installation Selections page opens.



17. Verify the Active Directory Certificate Services setup, and click Install.

The Installation Results page opens.



18. Verify that the installation has succeeded.
19. Click Close to close the Add Role Wizard.
20. Verify that the Server Manager now has an Active Directory Certificate Role.
21. Close the Server Manager.

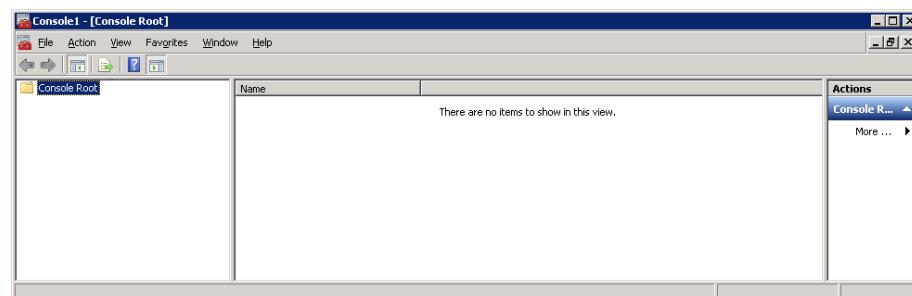
You have successfully added the active directory certification role to the Active Directory.

How to Create an AD Certificate File

Follow these steps:

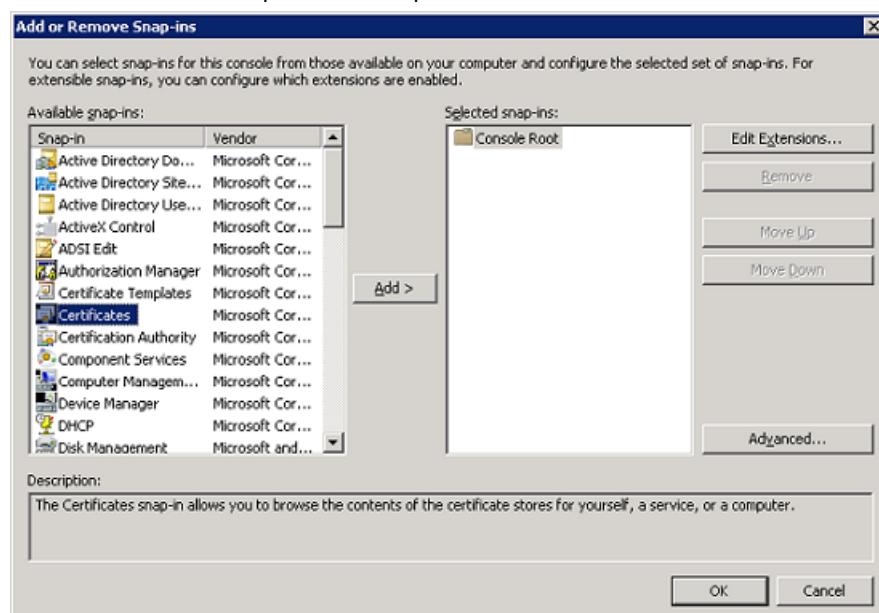
1. Open a Command Prompt using the option Run as Administrator.
2. Enter MMC and press Enter.

The Microsoft Management Console opens.



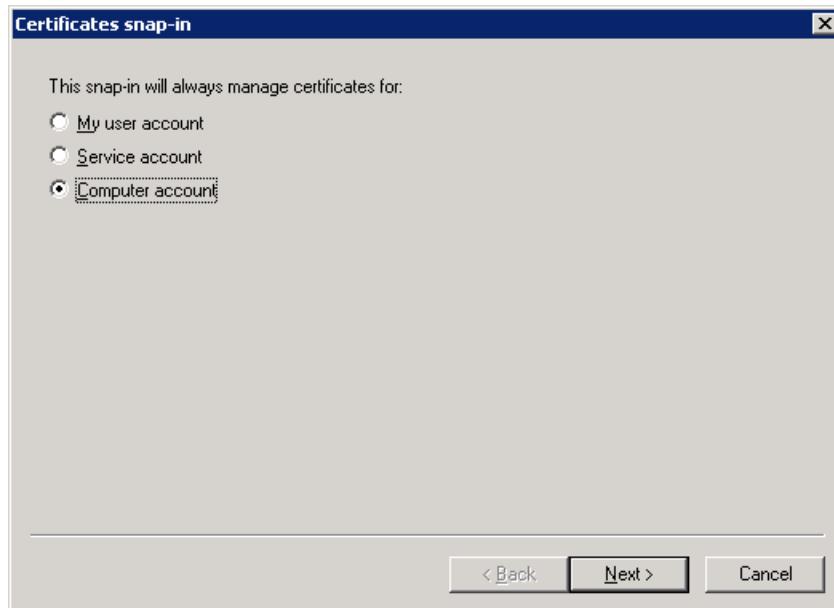
3. Select File from the toolbar and select Add/Remove Snap-in, from the drop-down list.

The Add or Remove Snap-ins wizard opens.



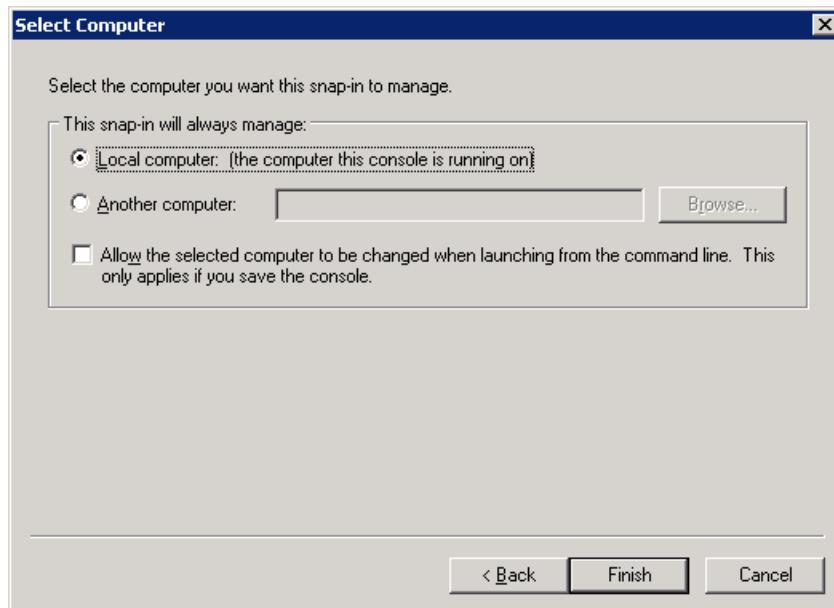
4. Select Certificate in the Available snap-ins section, click Add to move it to the Selected snap-ins section, and then click OK.

The Certificates snap-in page opens.



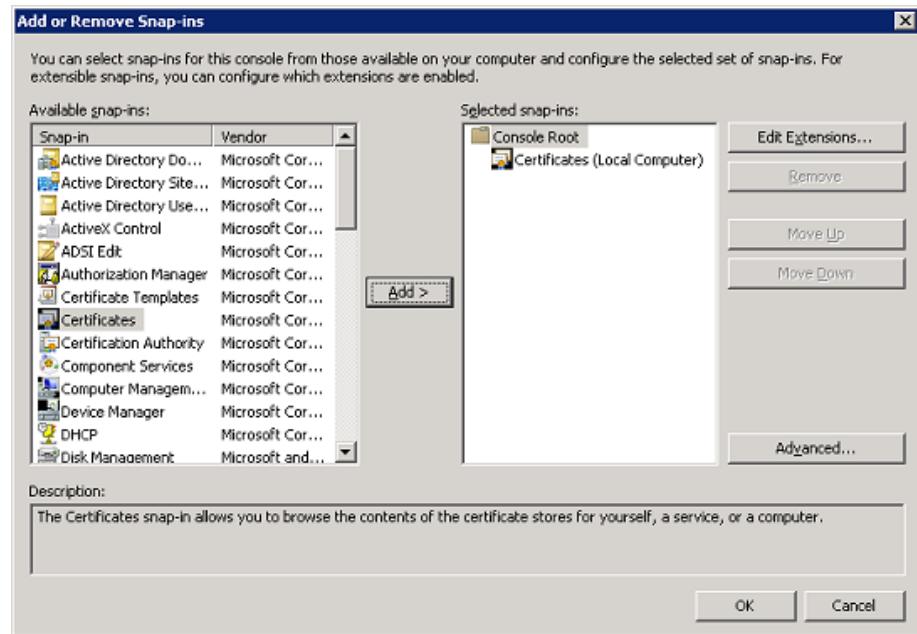
5. Select Computer account and click Next.

The Select Computer page opens.



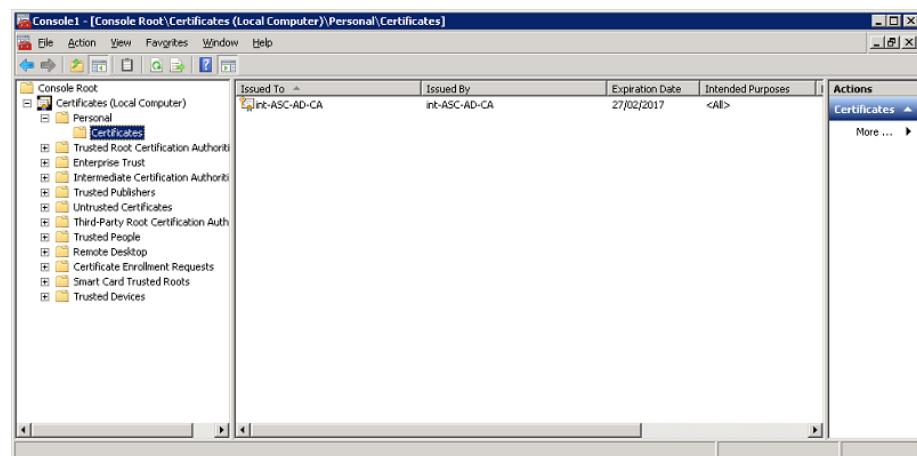
6. Select Local computer: (the computer this console is running on), and click Finish.

The Add or Remove Snap-ins page opens. The Certifications (Local Computer) is added to Selected snap-ins.



7. Click OK. The Add or Remove Snap-ins wizard closes.

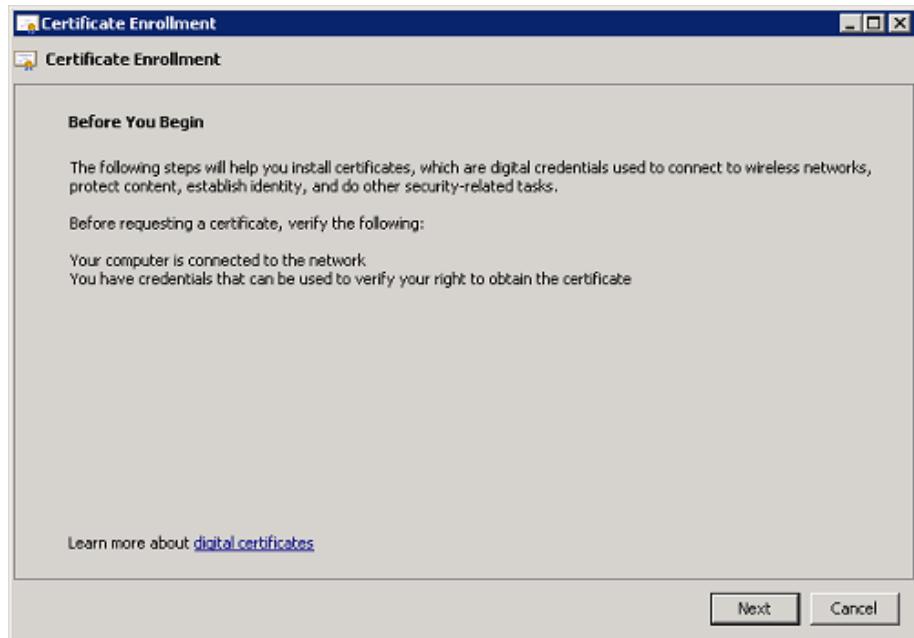
8. Expand Certificates (Local Computer) in the Console.



9. Expand Personal.

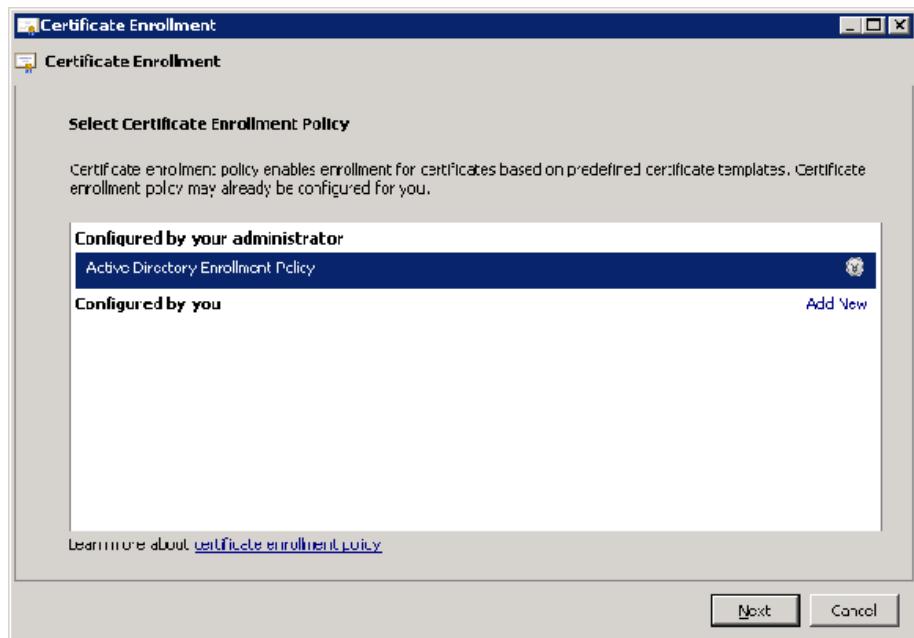
10. Right-click Certificates, select All Tasks, and then select Request New Certificate.

The Certificate Enrollment wizard opens.



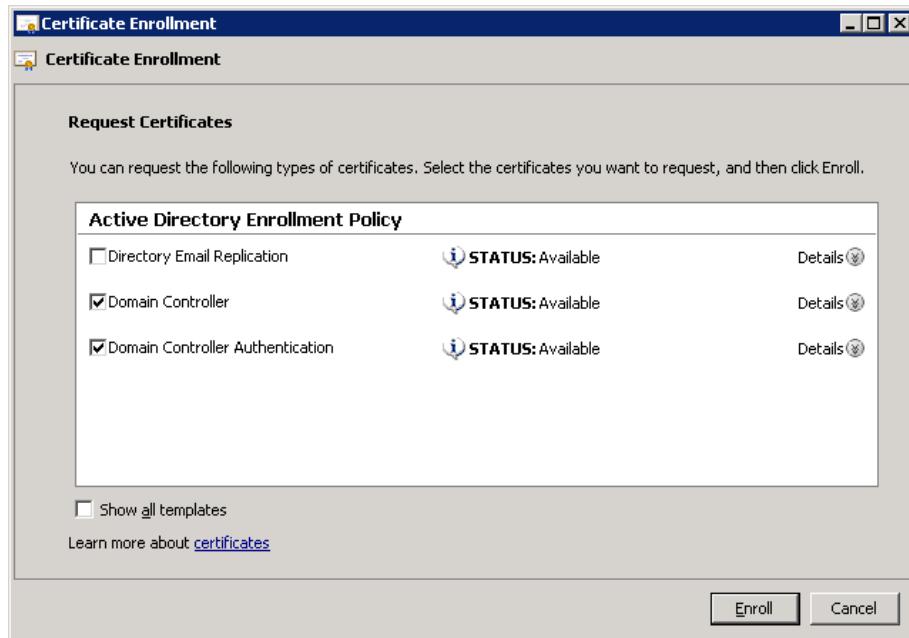
11. Read the instructions and click Next.

The Select Certificate Enrollment Policy page opens.



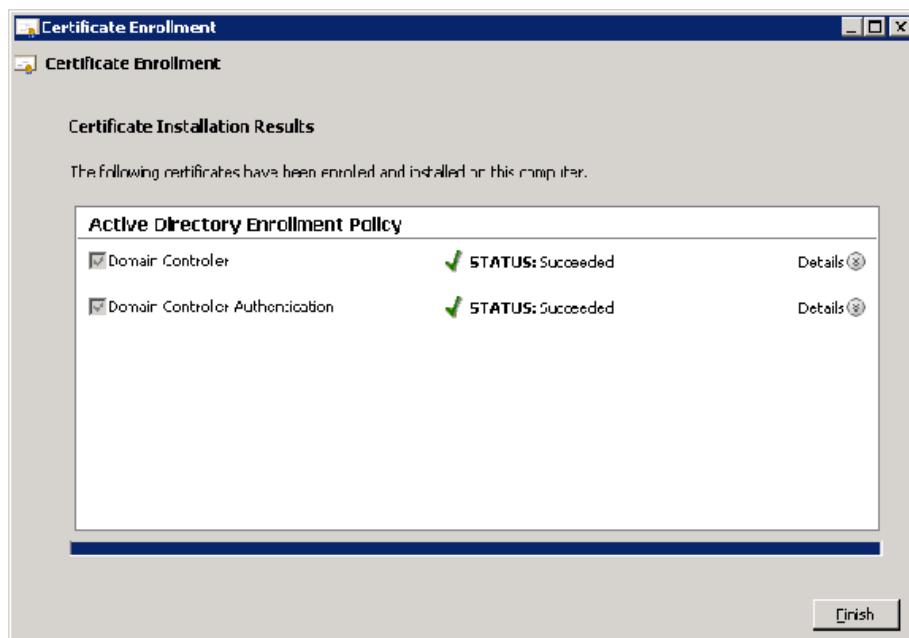
12. Verify that Active Directory Enrollment Policy is selected, and click Next.

The Request Certificates page opens.



13. Select Domain Controller, Domain Controller Authentication, and click Enroll.

The Certificate Installation Results page opens.

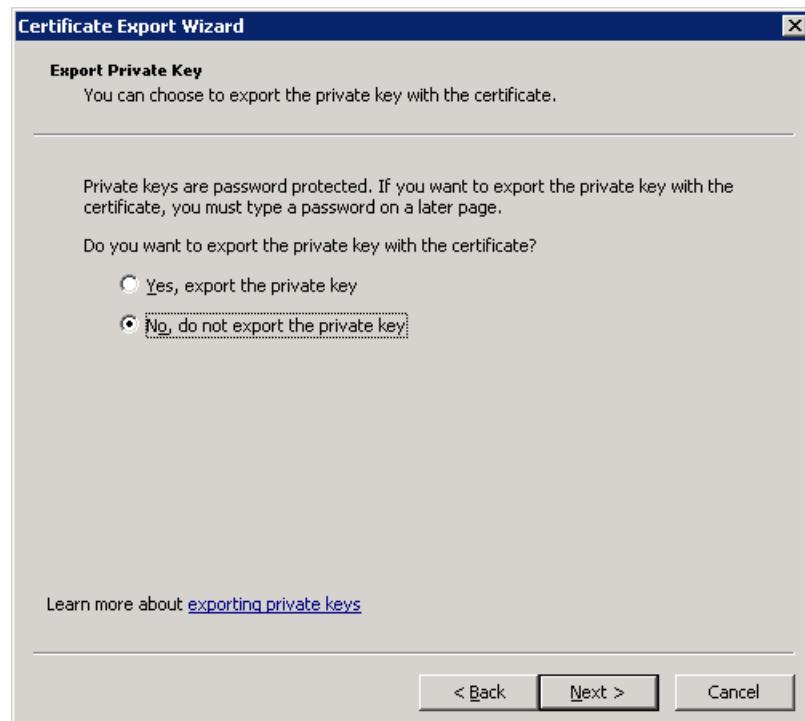


14. Verify that the status is Succeeded for both policies, and click Finish.

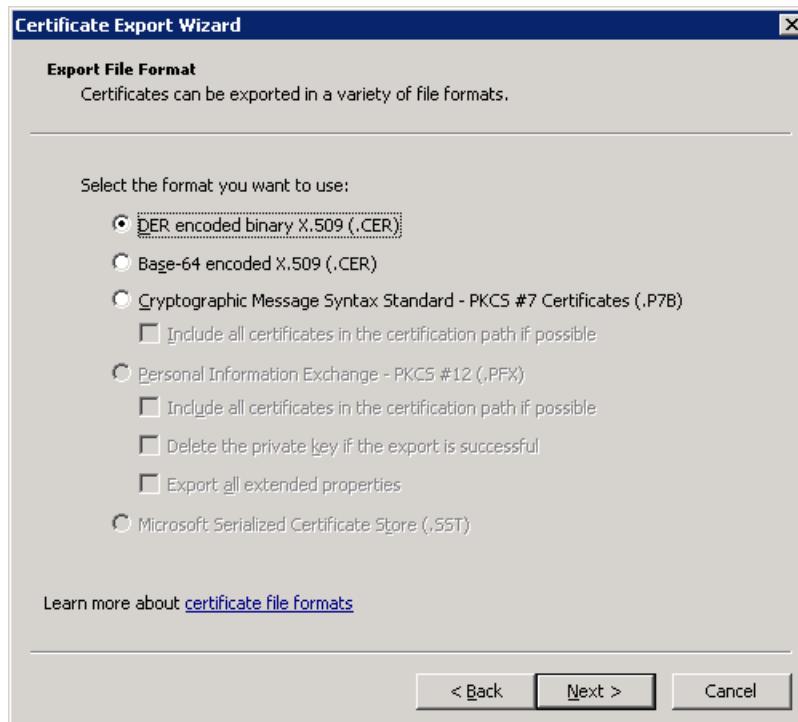
15. Verify that there are three certificates under Certificates, in the Console.
16. Right-click the certificate with the Intended Purpose of <All>.
17. Select All Tasks and Export.

The Certificate Export Wizard opens.

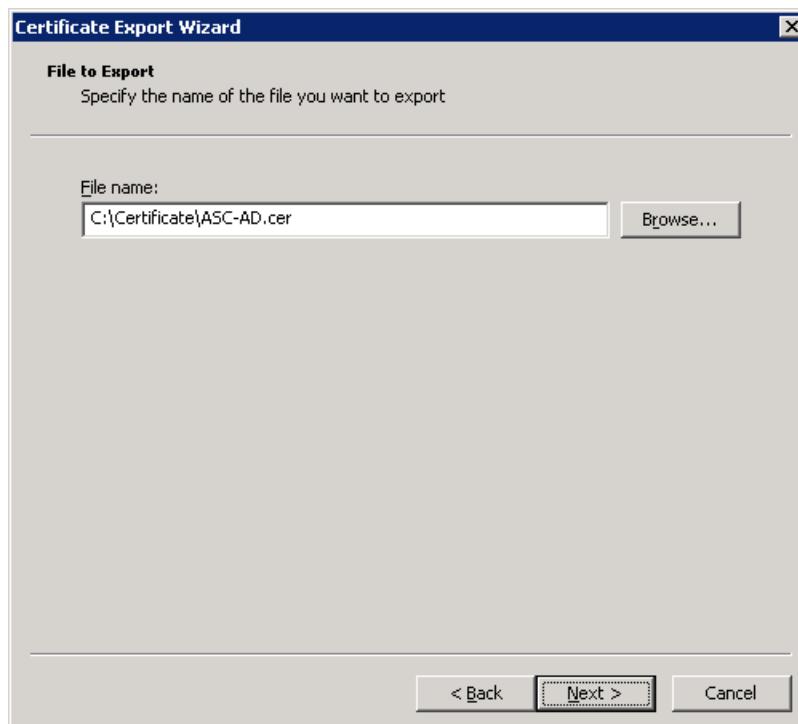
18. Click Next, to continue.



19. Select the option No, do not export the private key, and click Next.



20. Select DER encoded binary X.509 (.CER), and click Next.



21. Browse and create a folder named Certificate (\Certificate).
22. Name the certificate file to identify it (ASC-AD.cer) and click Next.

The Completing the Certificate Export page opens.



23. Verify the Certification Export information and click Finish.

A success message opens.



24. Click OK.
25. Close the Microsoft Management Console.

A save message opens.

26. Click Yes and Save to save the Console.

A Certification File (ASC-AD.cer) is created in the Certification folder on the Domain Controller.

Note: Copy the Certification File (ASC-AD.cer) to the CA Process Automation server.

Appendix B: Security Configuration

Allow Remote Connections through Windows Firewall

Follow these steps:

1. Open Server Manager.
2. Right-click Computer, and select Manage.
3. Expand Configuration.
4. Expand Windows Firewall with Advanced Security.
5. Highlight Inbound Rules.
6. Select New Rule, under Actions.

The New Inbound Rule Wizard opens.

- a. Select Port and click Next.
- b. Verify that TCP and Specific local ports are selected, enter the SQL port (1433), and click Next.
- c. Verify that Allow the connection is selected and click Next.
- d. Verify that the rule applies to all Profiles (Domain, Private, and Public), and click Next.
- e. Enter a Name for this Rule (SQL) and click Finish.

7. Verify the connection from a machine with only the SQL Client installed.

Turn off Internet Explorer Enhanced Security Configuration

We recommend turning off the Internet Explorer Enhanced Security Configuration (IE ESC). Turning off IE ESC allows Administrators and Users to open all CA Automation Suite for Clouds Solution User Interfaces (Web-based) without having to set and configure access.

Follow these steps:

1. Open the Server Manager.
2. Select Configure IE ESC.
3. Select Off for both Administrators and Users.
4. Click OK.

Turn on Windows 2008 Firewall

If Windows Firewall must be tuned on, Notifications must be enabled during the installation and configuration. Users are notified when a program encounters a blocked port. Create a permanent Windows Firewall Rule for allowing the program to communicate on the specific port and grant access to users.

Enable Notifications

Follow these steps:

1. Open Windows Firewall.
2. Go to Start, Run, and enter `firewall.cpl`.
3. Select Change Notification Settings.
4. Select Notify me when Windows Firewall blocks a new program.
5. Click OK.

Allow Access

When Notifications are enabled, the user is prompted the first time that a program attempts to access a protected port.

To allow access, click Allow Access. Windows Firewall creates a Rule and the program is permanently granted access on the required port.

Allow ICMP

Another Windows Firewall setting that you must adjust is to allow ICMP (PING) to work while checking communication between the various servers.

Follow these steps:

1. Open Windows Firewall.
2. Select Advanced settings.
3. Select Windows Firewall Properties.
4. Select the IPsec Setting tab.
5. Change the IPsec exemptions, Exempt ICMP from IPsec value from No (default) to Yes.
6. Click OK.
7. Close the Windows Firewall, and Windows Firewall Properties windows.

Appendix C: SQL Configuration

Install Microsoft SQL Server 2008 R2 Standard

Follow these steps:

1. Log in as the local Administrator or a user with administrative rights to the server.

2. Connect to the media.

Note: Version Used is en_sql_server_2008_r2_standard_x86_x64_dvd_521546.

3. Double-click SETUP.

4. Click OK, and wait until the SQL Server Installation Center opens.

Note: The following steps 5 – 8 can be skipped and you can go directly to Step 9 to start the installation.

5. Verify that Planning is selected (Bold).

6. Click the System Configuration Checker.

7. Verify that the status for Operation completed and Setup Support Rules is Passed. If the status is Failed, correct them. Warning issues must be corrected but are not required.

a. Click Show details to see issue details.

b. After the problem is corrected, click Re-run to run the Setup Support Rules again.

8. Click OK to close the System Configuration Checker.

9. Select Installation.

10. Click New installation or add features to an existing installation.

11. Verify that the status for Operation completed and Setup Support Rules is Passed. If the status is Failed, correct them. Warning issues must be corrected but are not required.

a. Click Show details to see issue details.

b. After the problem is corrected, click Re-run to run the Setup Support Rules again.

12. Click OK.

The Product Key page opens.

13. Enter the product key, and click Next.

14. Select the option I accept the license terms, and click Next.
15. Verify that no Setup Support Files are required.
16. Click Install.
17. A status bar appears with the status In Progress while the Setup Support Rules are checked.
18. Verify that the status for Operation completed and Setup Support Rules is Passed. If the status is Failed, correct them. Warning issues must be corrected but are not required.
 - a. Click Show details to see issue details.
 - b. After the problem is corrected, click Re-run to run the Setup Support Rules again.
19. Click Next.
20. Verify that SQL Server Feature Installation is selected, and click Next.
21. Select the following Features:
 - a. Database Engine Services
 - b. Client Tools Connectivity
 - c. (Optional) SQL Server Books Online
 - d. Management Tools - Complete
22. Change the Shared feature directories if you wish to change the installation location, and click Next.
23. Verify that the status for Operation completed and Installation Rules is Passed. Several rules have the Skipped status.
 - a. Click Show details to see issue details.
 - b. Click Re-run to run the Installation Rules again.
24. Click Next.
25. Verify that the Instance ID, and the Directory settings are correct, and click Next.
26. Verify that the Disk Space Requirements are checked, and click Next.
27. Click the drop-down field under Account Name and select NT AUTHORITY\SYSTEM for SQL Server Agent and SQL Server Database Engine.
28. Click Next.

29. Fill the following fields:
 - Select Mixed Mode and enter a password for the sa account.
 - Click Add Current User to add the local Administrator account.
 - Click Add to add additional accounts from the local or Domain user account database
30. Click Next.
31. Verify the Error Reporting page, and click Next.
32. Verify that the status for Operation completed and Installation Rules is Passed.
Several rules have the Skipped status.
 - a. Click Show details to see issue details.
 - b. Click Re-run to run the Installation Rules again.
33. Click Next.
34. Review the Ready to Install information.
35. Click Install. Click Close.
36. Close the SQL Server Installation Center.

Install SQL Server 2008 R2 Standard Client

This section describes the installation procedure for the R2 Version of SQL Server 2008. If you are installing earlier versions of SQL Server 2008, manually add the Feature Microsoft .NET Framework.

Follow these steps:

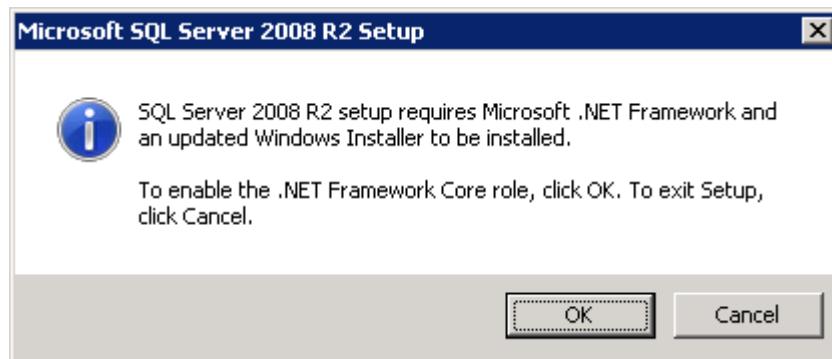
1. Open Server Manager, right-click Computer, and select Manage.
2. Highlight Features. Click Add Features.
3. Expand and check .NET Framework 3.5.1.
4. Click Next. Click Install.
5. Click Close.

Follow these steps:

1. Log in as the local Administrator or a user with administrative rights to the server.
2. Load Media.
 - Version: en_sql_server_2008_r2_standard_x86_x64_dvd_521546
 - Server: Local

3. Double-click SETUP.

A setup message appears.



4. Click OK. Wait until the SQL Server Installation Center opens.



You can perform the following procedures from the SQL Server Installation Center:

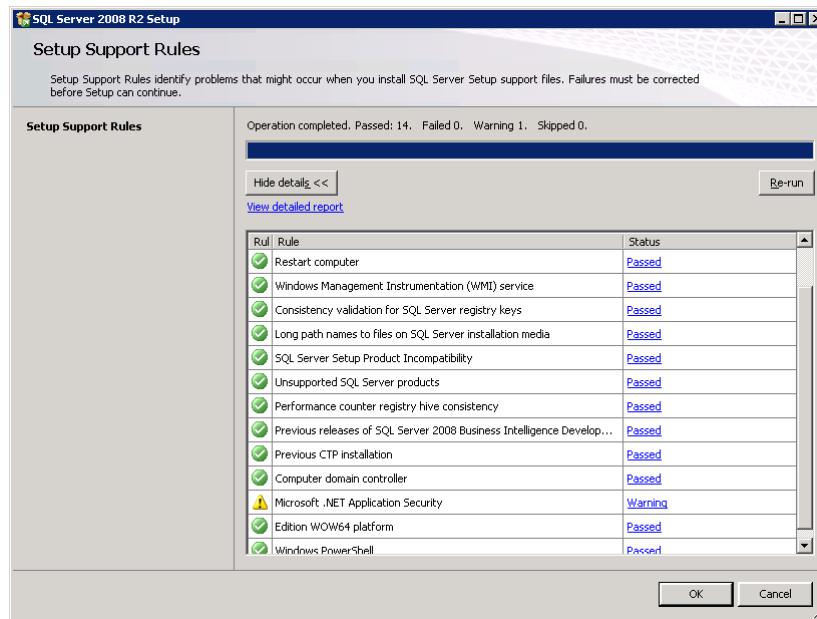
- Planning
- Installation

The following procedure lists the steps for planning the installation.

Follow these steps:

1. Select Planning in the SQL Server Installation Center page.
2. Click System Configuration Checker.

The Setup Support Rules page opens.



3. Ensure the status is Passed for Operation completed and Support Rules.

The rules with a Failed status must be corrected. Warning issues must be corrected but are not required.

- a. To correct a status, follow these steps:
 - Click Show details to see issue details.
 - After the problem is corrected, click Re-run to run the Setup Support Rules again.

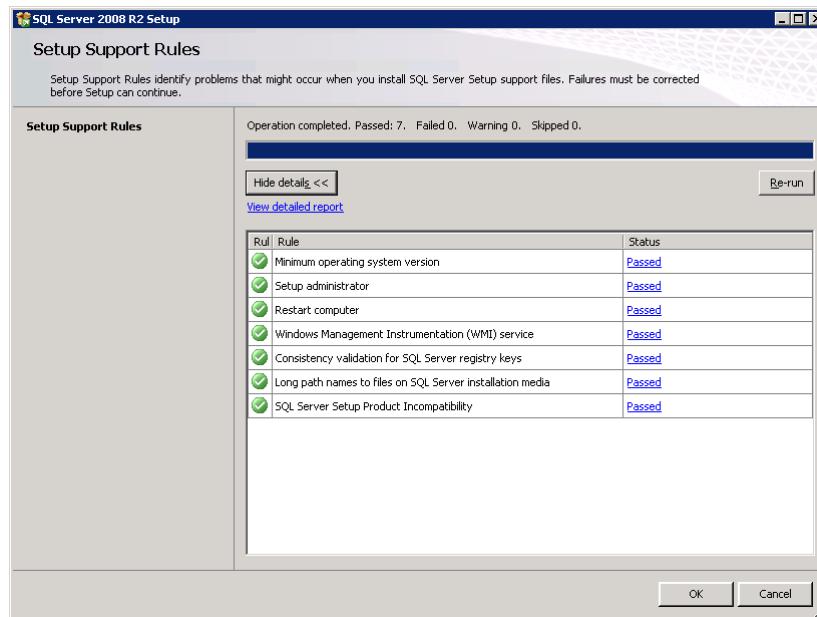
4. Click OK to close the System Configuration Checker.

The following procedure lists the steps for the installation.

Follow these steps:

1. Click Installation in the SQL Server Installation Center page.
2. Click New installation or add features to an existing installation.

The Setup Support Rules page opens.



3. Ensure the status is Passed for Operation completed and Support Rules.

The rules with a Failed status must be corrected. Warning issues must be corrected but are not required.

- a. To correct a status, follow these steps:
 - Click Show details to see issue details.
 - After the problem is corrected, click Re-run to run the Setup Support Rules again.

Note: Verify the status and make the corrections on every Setup Support Rules page.

4. Click OK.

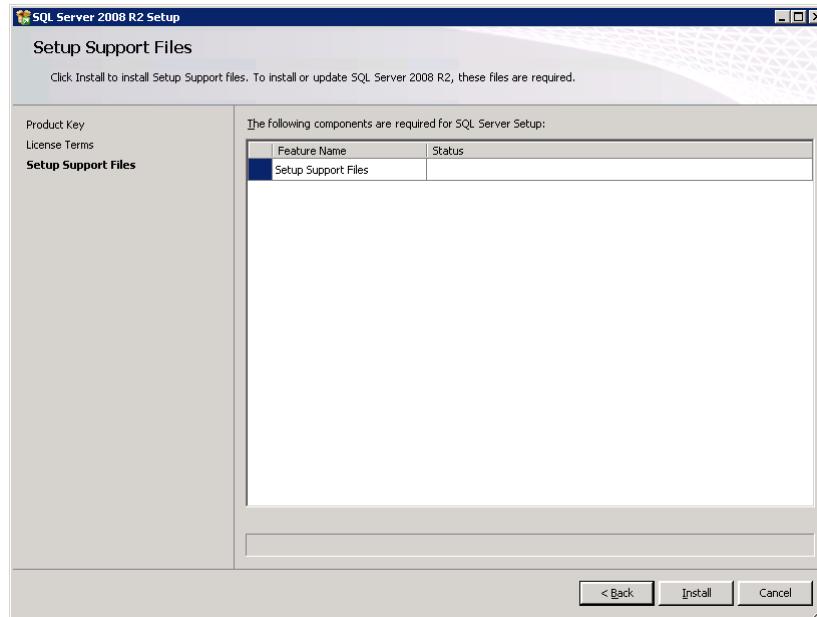
The Product Key page opens.

5. Type the product key, and click Next.

The License Agreement page opens.

6. Read the agreement, select I accept the license terms, and click Next.

The Setup Support Files page opens.



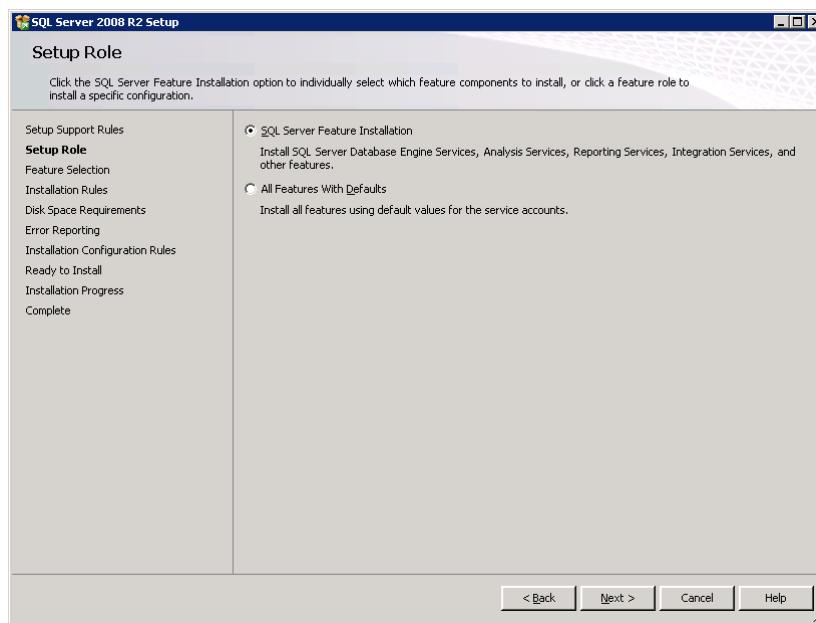
7. Verify that no Setup Support Files are required.

8. Click Install.

A status bar displays the progress of the installation. The Setup Support Rules page opens.

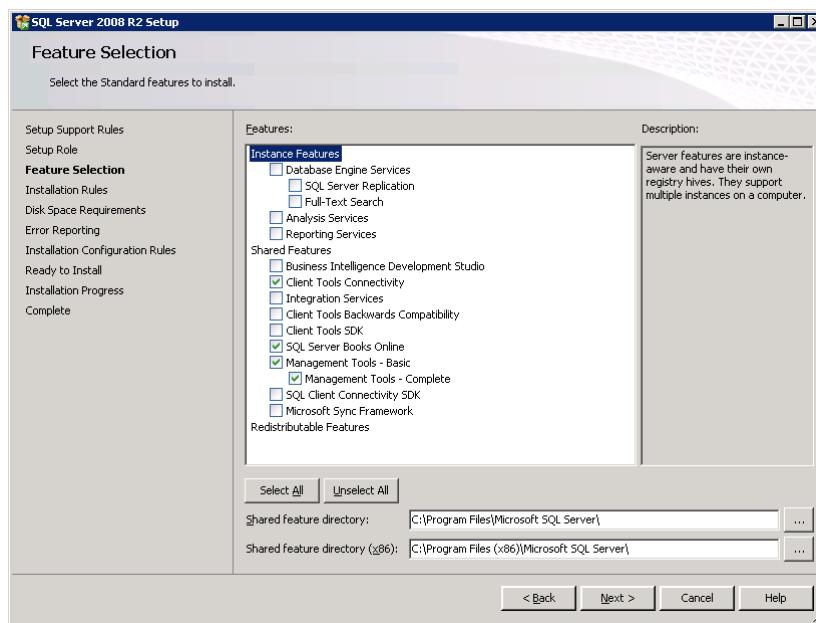
9. Verify the status and click Next.

The Setup Role page opens.



10. Select SQL Server Feature Installation, and click Next.

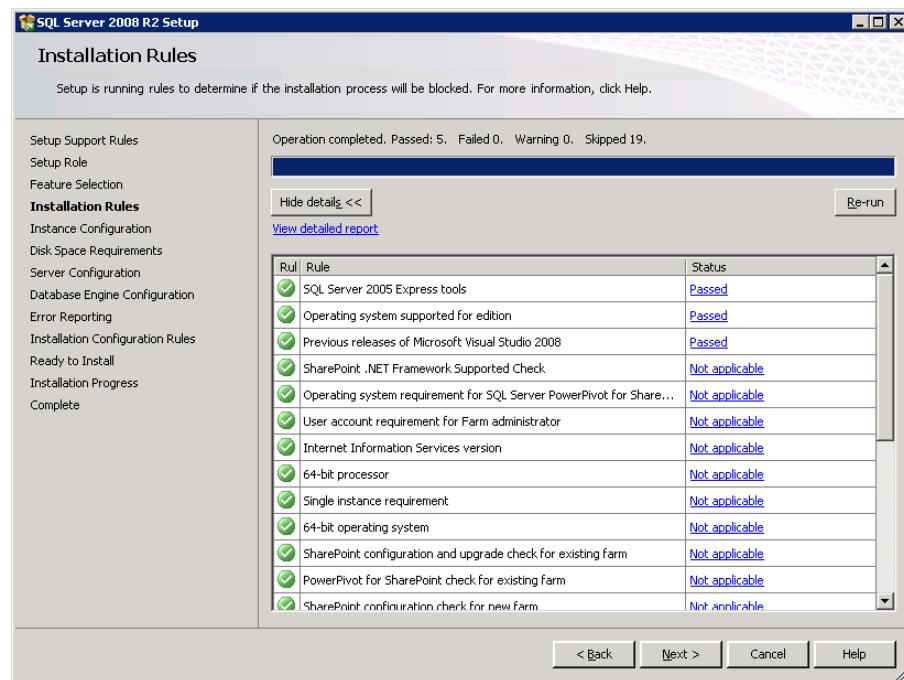
The Feature Selection page opens.



11. Select or change the following information:

- Select the following features:
 - Client Tools Connectivity
 - SQL Server Books Online (Optional)
 - Management Tools - Complete
- Change the Shared feature directory if you want to change the installation location.
- Click Next.

The Installation Rules page opens.



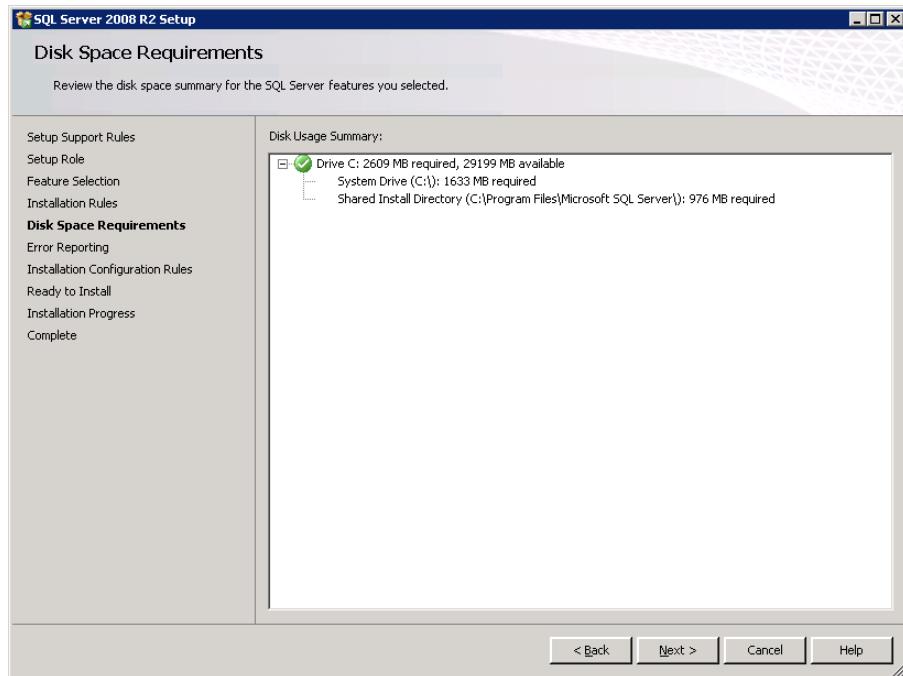
12. Ensure the status is Passed for Operation completed and Support Rules.

The status Skipped appears for several rules.

- Click Show details to see issue details.
- Click Re-run to run the Installation Rules again.

13. Click Next.

The Disk Space Requirements page opens.



14. Verify that the Disk Space Requirements are checked, and click Next.

The Error Reporting page opens.

15. Verify that the Select Windows check box is clear, and click Next.

The Installation Configuration Rules page opens.

16. Verify the status, and click Next.

17. Review the Ready to Install information, and click Install.

18. The Complete page opens.

19. Read the completion message, and click Close.

20. Close the SQL Server Installation Center.

Verify SQL Connectivity

Follow these steps:

1. Open Microsoft SQL Server Management Studio.
2. Enter the hostname of the SQL Server machine in the Server Name.
3. Change Authentication to SQL Server Authentication.
4. Enter the credentials for the SQL Administrator account (sa).

5. Click Connect.

Note: If the remote connection cannot be made, the following modification must be done to the SQL Server machines Windows Firewall.

How to Create an SQL Alias

Using an SQL Alias is required to connect an installation of SQL Server on a remote machine. In most cases, it is not needed but sometimes it is useful in the following circumstances:

- SQL Server is using a Port other than 1433
- SQL Server has a Named Instance which is using a Dynamic TCP/IP Port Number
- Name Resolution within the Domain makes connecting to the SQL Server difficult or impossible using the hostname (SERVERSQ121)

For example, DNS is not properly configured and the only way to PING the SQL Server machine is by using the IP Address or the Fully Qualified Hostname (serversql21.domain.com). During some product installation using the IP Address or Fully Qualified Hostname can cause problems or not be accepted. So to simplify the connection it is preferred that the communication work using the simple Hostname of the SQL Server machine or in this case Alias.

To connect to a remote SQL Server, the SQL Workstation component must be installed on the local machine. The Workstation component installs the Client Connectivity and the SQL Management Tools.

Follow these steps:

1. Click Program Files, Microsoft SQL Server 2008, Configuration Tools, and open the SQL Server Configuration Manager.
2. Expand SQL Native Client Configuration.
3. Right-click Alias, and select New Alias.
4. Complete the following fields:

Alias Name

Enter a SQL Server name to access the remote SQL Server from this computer.

Note: Use the hostname of the remote SQL Server.

Port No

Enter the Port being used to communicate with SQL Server.

Protocol

Keep TCP/IP unless a different Protocol is needed (Not Recommended).

Server

Enter the IP Address or Hostname (Fully Qualified if needed) that communicates successfully with the remote SQL Server.

To verify the SQL Alias, connect to the remote SQL Server Database using Microsoft SQL Server Management Studio. Use the Alias Name as the Server Name.

How to Determine the TCP/IP Port Number for a Named Instance of SQL

This procedure provides information about how to determine the TCP/IP port number for named instance of SQL from SQL Server:

Follow these steps:

1. Open SQL Server Configuration Manager.
2. Click SQL Server 2008 Network Configuration, Protocols for InstanceName.
3. Double-click TCP/IP in the right pane.
4. Click the IP Addresses tab.

You can make a note of the value of the TCP Dynamic Ports item under IPAll. Use the Port Number when creating a SQL Alias.

Appendix D: Upgrade CA ITCM r12.8 C1

See the Upgrade and Migration Considerations section in the *CA IT Client Manager Implementation Guide*. You can download the *CA IT Client Manager Implementation Guide* from the CA Automation Suite for Clouds bookshelf.