CA Process Automation

Installation Guide

Service Pack 04.0.01

technologies

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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- The organization of this book has been updated to better reflect the installation options you can select from the Installation palette in the Configuration tab, with their prerequisites. New sections include:
  - Adding a Node to the Domain Orchestrator (see page 97).
  - Installing an Additional Orchestrator (see page 105).
  - Adding a Node to an Additional Orchestrator (see page 113).
- A Simple Architecture (see page 11)—This new topic precedes an existing topic on a complex architecture. The new topic shows the minimum setup you need for a Domain Orchestrator.
- Prepare Microsoft SQL Server for CA Process Automation (see page 26)—This existing topic was edited. Although the driver name and the path name are unchanged, the installer has replaced the Microsoft SQL Server JDBC Driver 3.0 version with the 4.0 version.
- F5 Load Balancer Prerequisites (see page 41)—This new section addresses how you configure a load balancer for a clustered Orchestrator with the BIG-IP Configuration Utility, F5 Networks.
- Time Synchronization Prerequisites (see page 47) and Synchronize Time for a Cluster Node (see page 103)—These new topics include recommendations on how you can synchronize the internal clocks used by all Orchestrators and nodes in your network.
- Domain Orchestrator Installation (see page 49)—This existing topic was updated to include the new "embedded mode" option, which allows you to install CA Process Automation without first installing CA EEM or an external database.
- Resolve Invalid Character in CA Process Automation DNS Name (see page 126)—This new topic applies to users who are upgrading from r3.1, when CA Process Automation accepted DNS host names for Orchestrators that included invalid characters such as underscores. This new topic describes the corrective action.
- Using an Embedded Mode CA Process Automation (see page 135)—This new appendix describes the embedded database server and how to use the internal file-based authorization and authentication system.

Contents

Chapter 5: Upgrading to the Current Release 75

Chapter 6: Installing an Agent 87

Chapter 7: Adding a Node to the Domain Orchestrator 97

Chapter 8: Installing an Additional Orchestrator 105

Chapter 1: About this Guide

Click the link for the procedure you want to perform:

Initial Installation

Architecture and CA Process Automation Components (see page 11).

Platform Support and Hardware Requirements (see page 17).

Installing the Domain Orchestrator (see page 21).

Notes: After installing the Domain Orchestrator:

- See the first section in Online Help, "Task Flows by Role" for an overview of CA Process Automation.
- See the *Content Administrator Guide* for details on configuring CA Process Automation and setting up users in CA EEM.

Upgrade

Upgrading to the Current Release (see page 75).

Additions

Installing an Agent (see page 87).

Adding a Node to the Domain Orchestrator (see page 97).

Installing an Additional Orchestrator (see page 105).

Adding a Node to an Additional Orchestrator (see page 113).

Problems?

Troubleshooting (see page 129).

Other

Using CA SiteMinder with CA Process Automation (see page 119)

Using an Embedded Mode CA Process Automation (see page 135)

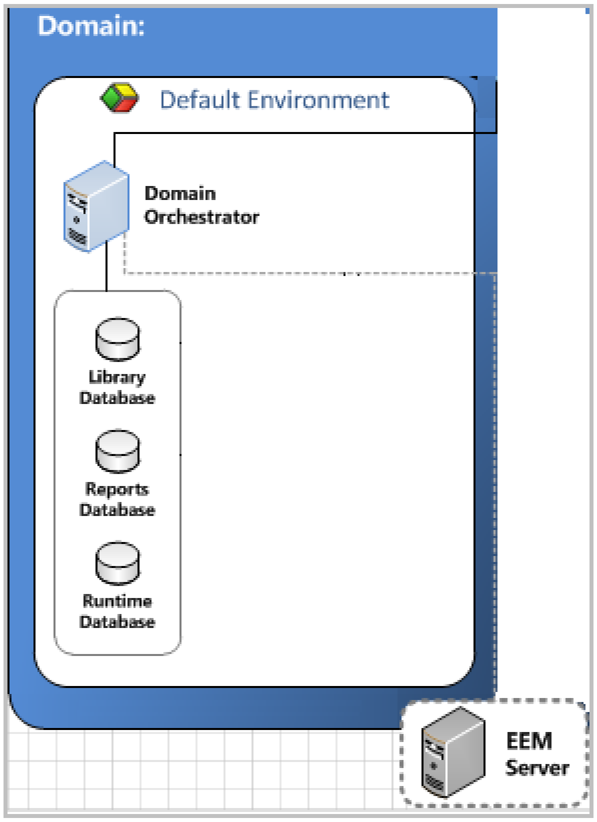
Chapter 2: Architecture and CA Process Automation Components

This section contains the following topics:

A Simple Architecture

A simple architecture is sufficient for many applications. A minimal CA Process Automation installation consists of:

- A single Domain Orchestrator.
- Three databases installed on the database server you specify. (Oracle, Microsoft SQL Server and MySQL are supported.)
- Access to a single CA Embedded Entitlement Management (CA EEM) server for user authentication and authorization to CA Process Automation.



Your first installation installs the CA Process Automation Domain with the Domain Orchestrator in the Default Environment. One Library database (Repository database) and one Reporting database are installed with the Domain Orchestrator; these databases can be shared with additional Orchestrators. The Domain Orchestrator includes a Runtime database. Each Orchestrator has its own Runtime database.

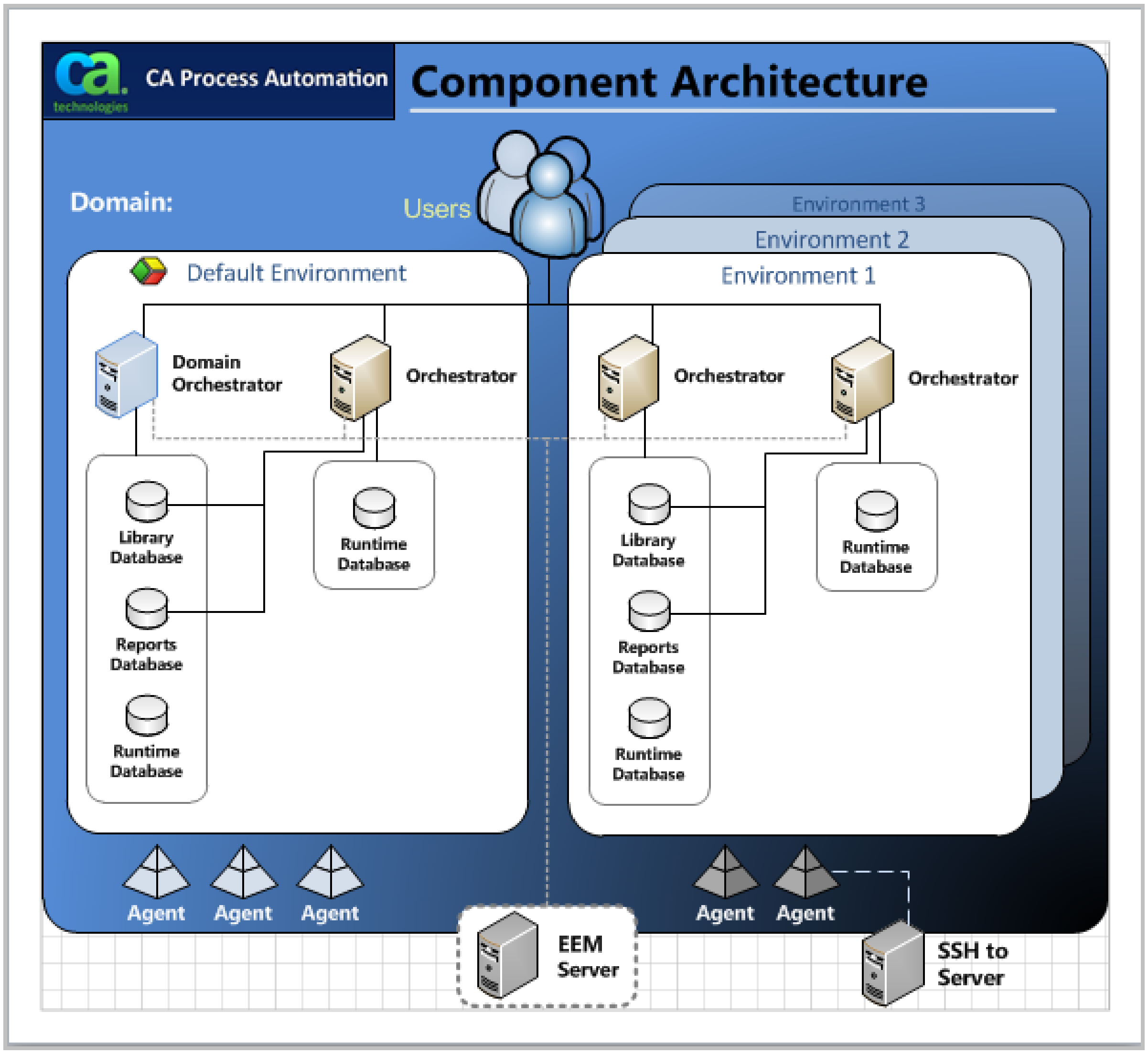
More information:

A Complex Architecture (see page 13)

A Complex Architecture

You can deploy CA Process Automation to meet high processing volume, high availability, and organizational requirements. The following illustration shows a CA Process Automation installation with the following components:

- A CA EEM server for the Domain.
- Multiple database servers, one per environment.
- The initial installation results, that is, the Default Environment with the Domain Orchestrator, a Library database, a Reports database, and a Runtime database.
- An Orchestrator that has been installed and added to the Default Environment, where this Orchestrator has its own Runtime database but shares the Library database and Reports database that were installed with the Domain Orchestrator. Optionally, you can set up an additional Orchestrator with its own Library database and Reports database.
- Additional Environments with Orchestrators.
- Agents, installed components on which operators can run.
- A remote host to which an agent has an SSH connection.
- Users with user accounts in CA EEM. When users log in, CA EEM authenticates that user and presents a browser-based UI appropriate for the associated role.


CA Process Automation
Component Architecture
Domain:
Users
Environment 3
Environment 2
Environment 1
Default Environment
Domain Orchestrator
Orchestrator
Orchestrator
Orchestrator
Library Database
Reports Database
Runtime Database
Runtime Database
Library Database
Reports Database
Runtime Database
Runtime Database
Agent
Agent
Agent
Agent
Agent
EEM Server
SSH to Server

Planning the Locations of Supporting Components

Part of planning a CA Process Automation system is determining what new components you can colocate on the same server with the CA Process Automation Domain Orchestrator and which ones to install on separate servers. Let us consider these components of a CA Process Automation network.

- JDK - must be colocated
- CA Embedded Entitlements Manager (CA EEM) - can be colocated, but not recommended
- Database servers for the CA Process Automation databases - can be colocated, but not recommended
- Load balancer (if planning to cluster) - cannot be colocated
- Other Orchestrators - cannot be colocated
- Cluster Nodes - cannot be colocated
- NTP server - external to network
- SiteMinder (optional)

Each cluster node and each Orchestrator is typically installed on a separate server. The NTP server can be external to the network.

For a lightly loaded CA Process Automation, you could install the following entities on the same server on which you installed the Domain Orchestrator:

- CA EEM.
- Database server for the Library, Reports, and Runtime databases.

Consider the following factors when determining whether to colocate entities or use multiple servers:

- Characteristics of the server.

  Major factors include the quantity and speed of CPUs, memory, disk storage and networks.

- Volume of processes.

  Consider not only the total number of processes, but also their max sustained rates during periods of peak activity.

- Process implementation.

  Not all processes are equal. Some processes have few operators, others have hundreds. Some processes contain many CPU intensive activities, while others spend most of their time waiting for events or user interactions. This variability makes it difficult to specify loading in terms of process volume/rate. Even at the finer granularity of operators, throughput varies.

- Required level of responsiveness.

  Real-time responsiveness is never attainable with the current implementation. However, even less stringent requirements factor into when more hardware for additional Orchestrators come into play. With a stringent SLA, the system needs more spare capacity so that the peak periods still perform well. Without an SLA, the system needs only sufficient capacity to cover the average load.

- Intensity of usage for shared components.

  Consider what else the CA EEM and the RDBMS are used for.

In anticipation of future growth, we recommend against colocating CA EEM and the database server with the Domain Orchestrator. The only sure way to determine when you have enough resources is by actual full load testing.

Prepare for Failover to a Standby CA EEM

Consider setting up two CA EEM instances in a High Availability configuration. If CA EEM is configured in this way, the primary CA EEM acts as the active security authorization server for CA Process Automation. The secondary CA EEM is the standby security authorization server. The secondary CA EEM mirrors the primary CA EEM. The two CA EEM instances can point to the same external directory.

CA Process Automation automatically and transparently fails over from the primary CA EEM to the secondary CA EEM if the primary CA EEM fails after CA Process Automation makes the initial connection. Failover occurs even if the primary server is initially down when you configure both CA EEM servers in CA Process Automation.

See the CA EEM documentation for the CA EEM version that is deployed at your site for information about how to set up CA EEM in a High Availability configuration. Additional information is available on the CA Process Automation Implementation Best Practices page (accessible through a Quick Link on the CA Process Automation Home tab).

Chapter 3: Platform Support and Hardware Requirements

This section contains the following topics:

Platform Support and Requirements for CA Process Automation Components

The following table summarizes the platforms that CA Process Automation components support.

Note: The listed operating system and software support can change over time. For the latest information about version support, see “Compatibilities” on support.ca.com.

CA Process Automation Component	Supported Operating Systems	Required Software	Other Requirements
Orchestrator	Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2 Solaris SPARC 10, 11 Red Hat Enterprise Linux 5x, 6.0, 6.1, 6.2 CentOS 6.2 SUSE Linux Enterprise Server 10, 11 SP1 HP-UX 11iv2, 11iv3 AIX 5.3, 6.1, 7.1	One of the following Java SE Development Kits (JDK) supported by your operating system. ■ For Windows, Solaris SPARC, and Linux: Oracle J2SE 1.6.23, 1.6.26, 1.6.27, 1.6.30 and 1.7 Development Kit (JDK) ■ For HP-UX, minimum requirement level for JDK is 1.6_04. ■ For AIX, IBM J2SE 1.6 Development Kit (JDK). **Note:** When the hardware and operating system support both 32-bit and 64-bit versions of the JDK, select the 64-bit version.	N/A

CA Process Automation Component	Supported Operating Systems	Required Software	Other Requirements
Agent	Microsoft Windows Server 2003, 2003 R2,2008, 2008 R2 Solaris SPARC 10, 11 Solaris x86 10 Red Hat Enterprise Linux 5x, 6.0, 6.1, 6.2 CentOS 6.2 SUSE 10, 11 SP1 HP-UX 11iv2, 11iv3 AIX 5.3,6.1, 7.1 Red Hat Enterprise Linux 6.2 for IBM System z Series SUSE Linux Enterprise Server (SLES) 11 SP1 for IBM System z Series	One of the following Java Runtime Environment (JRE) releases supported by the operating system. ■ For Windows, Solaris SPARC, and Linux: Oracle J2SE 1.6, 1.7 ■ For AIX, IBM JRE 1.6 ■ For HP-UX, minimum level is 1.6_04.HP J2SE 1.6 (JRE) (32-bit) for HP-UX. Do not use Java 6 Runtime Environment updates 27 (1.6.0_27) through 29 (1.6.0_29). An issue with those versions affects applications including CA Process Automation that use JDBC to connect to Microsoft SQL Server. The SDN bug database lists this issue as bug 7105007. **Note:** When the hardware and operating system support both 32-bit and 64-bit versions of the JDK, select the 64-bit version.	For proxy touchpoints and host groups, each remote host must run an SSHv2 server. A UNIX remote host must have ksh.
Database Server	See the vendor documentation for supported operating systems.	One of the following relational databases: ■ MySQL r5.5 ■ Microsoft SQL Server 2005, 2008, 2008 R2 ■ Oracle 10g or 11g R2	Enable XA support. See Database Server Prerequisites (see page 23) for detailed requirements.
Directory Server	See CA Embedded Entitlements Manager (CA EEM) documentation.	CA Embedded Entitlements Manager (CA EEM) 8.4 SP4 or CA EEM r12	N/A
Browser-based UI	N/A	One of the following browsers: ■ Microsoft Internet Explorer 9x ■ Google Chrome Release 17, 18 ■ Mozilla Firefox 4.*x* through 12.0 **Note:** If you use a Firefox or Chrome browser, disable the inline spell check feature to avoid unnecessary processing.	Enable JavaScript. Adobe Flash Player

Hardware Requirements

The following table provides the minimum hardware requirements for each CA Process Automation component:

CA Process Automation Component	Required Hardware
Orchestrator	■ Server class hardware running multiple CPUs or multiple core CPUs ■ 4-GB RAM ■ Minimum 40-GB free disk space required ■ Minimum 100-Mbps network connection (1000 Mbps recommended)
Agent	■ Host capable of running a supported OS ■ 2-GB RAM ■ 4-GB disk space
Database server	See vendor specifications. Additional storage as required for the databases being hosted. **Note:** We recommended a minimum of 40 GB for your databases.
CA EEM	See CA Embedded Entitlement Manager documentation.
Browser-based user interface	Any host capable of running a supported browser.

Note: The configurations could be for physical and virtual machines.

Chapter 4: Installing the Domain Orchestrator

The Domain Orchestrator is what is installed when you install CA Process Automation for the first time. Before you install the Domain Orchestrator, you must complete the prerequisites. You can install the Domain Orchestrator interactively with a wizard. Or, you can create a response file with values for parameters that have no defaults and then run the script to install the Domain Orchestrator silently. After installation, configure ports and firewalls. Then you configure CA Process Automation as described in the *Content Administrator Guide*.

This section contains the following topics:

Prerequisites to Installing the Domain Orchestrator

Before you begin, plan the initial installation. You can start small and incrementally expand your CA Process Automation instance over time. Minimum requirements include:

- Server on supported hardware w/ supported operating system, for example, Windows Server 2003 or Windows Server 2008 (32-bit or 64-bit)
- CA EEM: 8.4.244 and above
- JDK 1.6 or 1.7 (except 1.6.0_29)
- Database server, for example, Microsoft SQL Server 2005 or SQL Server 2008 (32-bit or 64-bit)

Consider implementing the following products for your first installation to prepare for later expansion:

- (Optional) A load balancer. Specifying the Domain Orchestrator as node1 in a load balancer prepares this Orchestrator for clustering. (Adding cluster nodes can be done when the need arises.)
- (Optional) Single Sign On (SSO) capability through CA SiteMinder.

You can plan your initial CA Process Automation installation.

Follow these steps:

1. Identify a host for the Domain Orchestrator that meets requirements.

   See the Orchestrator component in the following two topics:

   - Platform Support and Requirements for CA Process Automation Components (see page 18).
   - Hardware Requirements (see page 20).

2. Verify that the host for the Domain Orchestrator has a supported JDK, and if missing, download it.

   See JDK Prerequisites (see page 30).

3. Plan whether to locate supporting components on the host with the Domain Orchestrator.

   See Planning the Locations of Supporting Components (see page 15).

4. Identify the database server to host the Library, Reporting, and Runtime databases for the Domain Orchestrator.

   See the Database Server component in the following two topics:

   - Platform Support and Requirements for CA Process Automation Components (see page 18).
   - Hardware Requirements (see page 20).

5. Prepare the database server.

   See Database Server Prerequisites (see page 23).

6. Identify the host for CA EEM, if a CA EEM is not already in use with another CA Technologies product.

   See the Directory Server component in the following two topics:

   - Platform Support and Requirements for CA Process Automation Components (see page 18).
   - Hardware Requirements (see page 20).

7. Evaluate configuration options for CA EEM.

   See CA EEM Prerequisites (see page 32).

8. If CA EEM and an Apache load balancer are configured with CA SiteMinder, then prepare to configure CA Process Automation to use the SSO capability.

   See Using CA SiteMinder with CA Process Automation (see page 119).

9. Evaluate the need for a load balancer for the Domain Orchestrator. CA Process Automation supports two methods of balancing clustered Orchestrators.

   See Apache Load Balancer Prerequisites (see page 34).

   See F5 Load Balancer Prerequisites (see page 41).

Database Server Prerequisites

CA Process Automation requires that you have one of the following third-party database servers in which CA Process Automation can store and persist its data:

- MySQL Server 5.5
- Microsoft SQL Server
- Oracle Database

If you do not have a server for CA Process Automation, download one with its prerequisites. We recommend that the database server and CA Process Automation reside on separate hosts.

Follow the guidelines for the database server you are using for the Orchestrator you are installing.

- Prepare MySQL Server for CA Process Automation (see page 25).
- Prepare Microsoft SQL Server for CA Process Automation (see page 26).
- Prepare Oracle Server for CA Process Automation.

About CA Process Automation Databases

Each Orchestrator requires three logical databases in its associated database server:

- The Repository database, or *Library database*, is a database that stores the automation objects created in folders in the Library tab in CA Process Automation. The stored data includes the library tree structure, the complete definition of each object, as well as ownership, and versioning information.

  Note: Multiple Orchestrators can share the Repository database on the Domain Orchestrator or each Orchestrator can have its own.

- The *Runtime database* is an Orchestrator-specific database that stores process instance data for a single Orchestrator. Data includes information on currently running process instances, instances that have been run but have not yet been moved to the archive table, and archived instances. You can access current and archived data from the Operations tab. Each runtime record includes the state, dataset, and owner for the object instance, as well as scheduling information.

  Note: Each Orchestrator requires a separate Runtime database.

- The *Reporting database* stores historical data for automation object instances, including processes, resources, schedules, process watches. Administrators can generate near real-time reports with this data using the predefined report definitions and custom report definitions in the Reports tab.

  Note: The Reporting database is typically shared among all Orchestrators.

These logical databases can share a physical database but the best practice is to have separate databases. CA Process Automation requires databases to be case insensitive.

We recommended a minimum of 40 GB for your databases. Specific operations such as upgrading CA Process Automation make unusually large demands. Having ample space and periodically monitoring space consumption is a good practice.

Depending on your CA Process Automation archiving policy, your runtime databases grow as processes run and are archived. You can set an archive purging policy to delete older records automatically, or you can perform this maintenance task outside of CA Process Automation.

Note: See Configure Orchestrator Policies in the *Content Administrator Guide*.

Prepare MySQL Server for CA Process Automation

During installation of the Domain Orchestrator or an additional Orchestrator, the installer creates CA Process Automation databases in the specified MySQL server. The installer requires the following:

- A MySQL JDBC driver that supports XA.

  During installation, you must browse to this driver. This driver is not included in the CA Process Automation installation media. MySQL database servers support XA distributed transactions by default.

- User credentials with Administrative privileges to create the Library, Reporting, and Runtime databases.
- Two MySQL variables customized for CA Process Automation.

Before you install an Orchestrator that uses the MySQL database server, you must make preparations.

Follow these steps:

1. Download the JDBC driver from the MySQL website. For example, get the MySQL Connector/J 5.0.8.

   Note: The MySQL Connector/J 5.0.x, a JDBC driver, supports XA directly.

2. Save the driver to a location that you can browse to during installation.
3. Open the MySQL Workbench and select the Options File under Configuration.
4. Set the variable for the time a transaction waits for a lock before being rolled back:
   a. Select the InnoDB tab.
   b. Scroll to the Various group.
   c. Select innodb_lock_wait_timeout.
   d. Change the value from the default, 50, to a value greater than 60.

   ```
   innodb_lock_wait_timeout = 90
   ```

5. Increase the maximum packet length to send to the server and receive from the server. The default is 1048576
   a. Select the Networking tab.
   b. Locate the Data / Memory size group.
   c. Select max_allowed_packet.
   d. Enter a value greater than the default.
6. Click Apply.

   A confirmation of the changes to apply to the MySQL Configuration File appears.

Prepare Microsoft SQL Server for CA Process Automation

Before installing the CA Process Automation Domain Orchestrator or an additional Orchestrator, where the CA Process Automation databases reside on SQL Server, do the following:

- Verify that the SQL Server meets CA Process Automation requirements (see page 26).
- Understand how the JDBC 4.0 driver is referenced (see page 27).
- Enable XA support for the SQL Server (see page 27).

Verify that the SQL Server Meets CA Process Automation Requirements

The SQL Server you prepare for CA Process Automation databases must meet the following requirements:

- SQL Server must be installed or configured with mixed mode authentication. You specify an account with SQL Server authentication during the Orchestrator installation.
- The Orchestrator installer requires user credentials with Administrator privileges to create the CA Process Automation databases.
- SQL Server collation for CA Process Automation databases must be SQL_Latin1_General_CP1_CI_AS. By default, the CA Process Automation installer creates databases with this collation.

Examine the configuration file for your SQL Server to verify that your SQL Server meets CA Process Automation requirements.

Follow these steps:

1. Navigate to the ConfigurationFile.ini file, which is created in a path similar to the following:

   ```
   C:\ Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\ yyyymmdd_hhmmss
   ```

2. Verify that the security mode setting resembles the following:

   ```
   ; 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:

   ```
   ; Windows account(s) to provision as SQL Server system
   administrators.
   SQLSYSADMINACCOUNTS=".\Administrator"
   ```

4. Verify that the setting for collation resembles the following:

   ```
   ; Specifies a Windows collation or an SQL collation to use for the
   Database Engine.
   SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
   ```

Understand How the JDBC 4.0 Driver Is Referenced

During installation of the Orchestrator, the installer requires the JDBC 4.0 driver for SQL Server, which is included in DVD1. The path is:

```
.../DVD1/thirdparty/mssql/sqljdbc_3.0/enu/sqljdbc.jar
```

Note: The path and jar file name have not been changed since JDBC 3.0 driver was used. That is, sqljdbc4.jar has been renamed to sqljdbc.jar. Use the jar file included in the installation media; it contains the JDBC 4.0 driver for SQL Server.

Enable XA Support for the SQL Server Before Initial Installation

The JBoss release that the CA Process Automation server runs on requires support for Extended Distributed Transactions (XA) at the database level. Microsoft SQL Server must be configured to support and enable XA transactions.

Brief definitions of XA-specific terms used in this topic:

XA - The term XA stands for eXtended Architecture.

XA transactions - XA transactions are global transactions that span multiple transaction resources. A non-XA transaction involves one resource, such as one database.

Microsoft JDBC Driver 3.0/4.0 for SQL Server - The two JDBC drivers that support XA on SQL Server.

xa_install.sql - The script that installs the extended stored procedures that implement distributed transaction and XA support for the Microsoft SQL Server JDBC Driver 3.0.

SQLJDBC_XA.dll - The file that must be copied from the JDBC installation directory to the Binn folder of every SQL Server that participates in distributed transactions. Copy this file before running the xa_install.sql script.

SqlJDBCXAUser - A SQL Server role. To grant permissions to *pamuser* to participate in distributed transactions with the JDBC driver, add the user to the SqlJDBCXAUser role.

By default, XA distributed transaction support is not enabled for Microsoft SQL Server. You can enable the XA support that CA Process Automation requires.

Follow these steps:

1. Navigate to the paths for your operating system:

   ```
   DVD1\thirdparty\mssql\sqljdbc_3.0\enu\xa\x64
   DVD1\thirdparty\mssql\sqljdbc_3.0\enu\xa\x86
   ```

   This directory contains the sqljdbc_xa.dll file.

2. Copy the sqljdbc_xa.dll file to the Binn directory of the SQL Server installation. For example:

   mssql_install_dir\MSSQL10.MSSQLSERVER\MSSQL\Binn

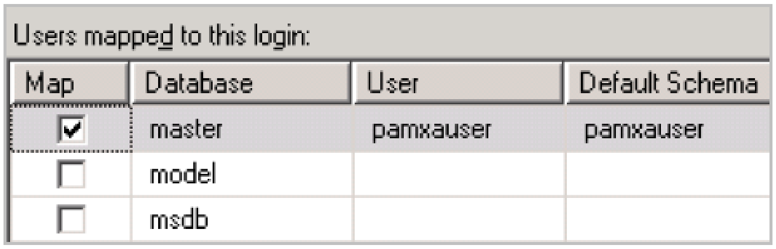
   mssql_install_dir\MSSQL.1\MSSQL\Binn

3. Restart the SQL Server.

4. Create a non-‘sa’ account for CA Process Automation to use to access its internal databases.

   a. Log in to the master database in SQL Management Studio.

   b. Create a user (for example, *pamxauser*) and assign **master** as the default database. Click OK



Users mapped to this login:

Map	Database	User	Default Schema
☑	master	pamxauser	pamxauser
□	model		
□	msdb		

   c. Select the *pamxauser*

   d. In the User Mappings, verify that the **public** database role is assigned to the master database. Click OK.

   e. In the Server Roles, verify that **public** is selected and select **dbcreator**. Click OK.

   f. Select File, Save All.

   g. Select File, Exit

5. Enable XA transactions for Distributed Transaction Coordinator.

   For Windows 2008

   a. From the Start menu, select Administrative Tools, Component Services.

   b. Expand Component Services, Computers, My Computer, and Distributed Transaction Coordinator.

   c. Right-click Local DTC and select Properties.

   d. Select the Security tab and select Enable XA Transactions.

   For Windows 2003

   e. Navigate to Administrative Tools, Component Services.

   f. Right-click My Computer and select Properties.

   g. Click the MSDTC tab.

   h. Click the Security Configuration button under Transaction Configuration.

   i. In the Security Configuration window, select Enable XA Transactions.

   j. Click Apply, click OK. Close Component Services.

6. Open Microsoft SQL Server Management Studio as the ‘sa’ user.

   a. Select File, Open, File and then browse to the xa_install.sql script.

      ```
      DVD1\thirdparty\mssql\sqljdbc_3.0\enu\xa\xa_install.sql
      ```

   b. Click Execute to run the script and load the DLL.

      Note: Ignore the permissions message similar to the following message:

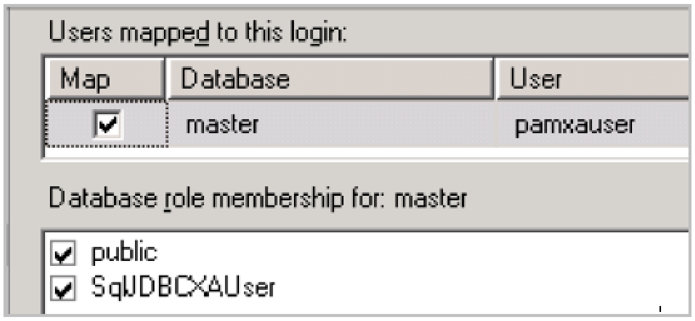
      > Msg 3701, Level 16, State 15, Procedure sp_dropextendedproc, Line 18
      > Cannot drop the procedure ‘xp_sqljdbc_xa_init’, because it does not exist or you do not have permission.

7. Run the following SQL commands to grant master database access to pamxauser and to add the SqlJDBCXAUser role to the master database.

   ```
   use master
   go
   exec sp_grantdbaccess 'pamxauser','pamxauser'
   go
   exec sp_addrolemember [SqlJDBCXAUser],'pamxauser'
   ```

   Note: An error message indicates that the user exists. Ignore this message.

8. Verify that the SqlJDBCXAUser role is selected for the *pamxauser* user for the master database, then exit Management Studio.



Users mapped to this login:

Map	Database	User
☑	master	pamxauser

Database role membership for: master

☑ public
☑ SqlJDBCXAUser

9. Restart your SQL Server.

   Coordinate with other users of the Database Server.

JDK Prerequisites

Before you install any Orchestrator, verify that the Java SE Development Kit (JDK) prerequisites are met. If the JDK you need is not present, download it.

Follow these steps:

1. Log in to each host where you plan to install the Domain Orchestrator.
2. Verify that an appropriate version of a Java Development Kit exists.
   - For AIX, Java 1.6 is required.
   - For all other platforms, Java SE Development Kit (JDK) 1.6 or 1.7 is required.

   Note: For other details, see Platform Support and Requirements for CA Process Automation Components.
3. If the required JDK version is not installed, obtain it from the vendor. Free downloads are available from IBM (AIX JDK), and Oracle (other platforms).
4. Run the installation wizard to install the JDK. Select all the defaults, for example, Development Tools, Source Code, and Public JRE.

Prepare an Oracle Database Server for CA Process Automation

Before you install the Domain Orchestrator or an additional Orchestrator that uses Oracle to host its internal databases, preparation is required.

Follow these steps:

1. Create a user with connect and resource permissions.
2. Verify that Oracle has sufficient table space to host the following databases:
   - Library database
   - Runtime database
   - Reporting database
3. Create the Library, Reporting, and Runtime databases manually.
4. Configure the following settings:
   - Set maximum connections to 100 (or at least 150 for clustered).

     All connections are made through Orchestrators, but a few pooled connections are required for optimal behavior.
   - Set Online Transaction Processing (OLTP) to facilitate transactions.
5. Understand how the JDBC 4.0 driver is referenced.

   During installation of the Orchestrator, the installer requires the JDBC 4.0 driver for Oracle, which is included in DVD1. The path is:

   ```
   .../DVD1/Drivers/ojdbc14.jar
   ```

Notes:

- Partitioning is *not* supported.
- No action is needed to enable XA distributed transactions, since Oracle supports it by default.

More information:

Oracle DBMS May Return Corrupted Data (see page 129)

CA EEM Prerequisites

CA Process Automation uses CA Embedded Entitlements Manager (CA EEM) for user authentication and authorization. CA EEM is a required prerequisite.

If you are using CA EEM with another CA Technologies product, check to see if it is a version supported by CA Process Automation.

- If you do not have CA EEM or if your CA EEM is an earlier version than the versions that CA Process Automation supports, then download and install CA EEM (see page 33).
- If your CA EEM is a version that CA Process Automation supports, gather information for the Domain Orchestrator installation (see page 33).
- To create two CA EEM instances at installation (one to use and the other as a standby for failover), see Prepare for Failover to a Standby CA EEM (see page 16). This procedure is optional and can be performed at a later time.
- If you are upgrading and you previously used AD or LDAP as your directory server, you can configure CA EEM to use AD as an external user store. With this approach, your existing user accounts are loaded into CA EEM during upgrade. Alternatively, you can use CA EEM directly, create user accounts, and assign each user one of the four default roles.

Download and Install CA EEM

If you are not using CA EEM with other CA Technologies products, you can download CA EEM and install it. If you are using a CA EEM version that CA Process Automation does not support, upgrade CA EEM.

Guidelines follow:

1. Log in to CA Support.
2. Download the CA Embedded Entitlements Manager (CA EEM) software. Select a release supported by the current release of CA Process Automation. See the Directory Server entry in Platform Support and Requirements for CA Process Automation Components (see page 18).
3. Download the CA EEM documentation.
4. Run the CA EEM installer.

Notes:

- When you configure CA EEM for CA Process Automation, you select whether to use the default user store or in an external user store such as Microsoft Active Directory. If you select the default user store (preferred), you can create user accounts for CA Process Automation users. If you point to an external user store, then user accounts from that store are automatically loaded into CA EEM as global users.
- CA Process Automation encrypts the data that is transported between CA Process Automation and CA EEM. If FIPS mode is selected in CA EEM, then you can select to use or not to use FIPS-supported algorithms for communication between CA Process Automation and CA EEM.

Gather Information for the Domain Orchestrator Installation

Whether you install CA EEM or use an existing CA EEM, have at hand the following details of your CA EEM configuration when you begin the installation of the Domain Orchestrator.

CA EEM Server

Specifies the host name where your CA EEM server is installed.

Within CA EEM, click Configure, then click Failover Information. The Hostname of the CA EEM server is displayed.

CA EEM Application Name

Specifies the name to assign as the application name for CA Process Automation.

Default: Process Automation

CA EEM Certificate File

Specifies the Certificate File. Accept the default value.

Defaults:

FIPS enabled: PAM.cer

FIPS disabled: PAM.p12.

Certificate Key File

During registration, a certificate key is provided if CA EEM is configured for FIPS mode.

Default: PAM.key

CA EEM Certificate Password

Specifies the CA EEM Certificate password.

Important! You must be able to provide the CA EEM Certificate password to successfully install CA Process Automation.

FIPS Mode

Specifies whether you want to use FIPS mode for CA Process Automation. True is valid only if you installed CA EEM with FIPS mode set to On.

Values: True, False

Note: The isFIPSMode() method returns "true" if the CA EEM server is running in FIPS mode. See the *Web Services Reference* for details on web service methods.

Important! You must know the password for the EiamAdmin user to log into CA EEM.

Apache Load Balancer Prerequisites

A *clustered Orchestrator* is a set of nodes that appear and act as a single Orchestrator and use a shared library. You can cluster any CA Process Automation Orchestrator for high availability, fault tolerance, and scalability.

A load balancer, such as the Apache HTTP Server, is required for clustering any Orchestrator, including the Domain Orchestrator. A load balancer is not part of the CA Process Automation installation.

While the load balancer can be configured on the same host as one of the Orchestrator nodes, it is more typical for the load balancer to reside on a separate host.

A load balancer is *only* required for an Orchestrator in a clustered configuration and in specific Single Sign On (SSO) configurations.

Important! If an Orchestrator is installed without first installing and configuring a load balancer, you cannot cluster that Orchestrator later.

The installation and configuration instructions in this section are specific to the Apache load balancer.

Note: You can use a load balancer other than Apache. However, a CA Process Automation Orchestrator requires that some classes of request be directed to a specific node in the clustered Orchestrator. Therefore, simple load balancing is insufficient. See the CA Process Automation Best Practices page, or contact CA support for assistance with alternatives. The Bookshelf includes links to these pages.

Follow these steps:

1. Install a load balancer and prepare configuration templates (see page 35).
2. Configure basic communication (see page 37).
3. (Optional) Configure secure communication (see page 37).

Install a Load Balancer and Prepare Configuration Templates

The CA Process Automation installation media includes sample configuration files for the Apache load balancer that you can use as a starting point for configuration.

- Non Secure Domain Orchestrator or Orchestrator

  `NonSecureDomainAndOrchestratorConfig_Template.zip`
- Secure Domain Orchestrator

  `SecureDomainConfig_Template.zip`
- Secure Orchestrator

  `SecureOrchestratorConfig_Template.zip`

The following instructions assume that an Apache 2.2 load balancer is dedicated to CA Process Automation. First, install an Apache load balancer. Then, extract files from the CA Process Automation ApacheConfTemplates zip file to the Conf folder under the Apache installation folder.

Follow these steps:

1. Log in to the host where the load balancer is to run.

   The load balancer typically is not on the same host as your Domain Orchestrator. However, the host with your Domain Orchestrator must be routable from the load balancer.

2. Download and install the latest Apache load balancer with SSL support. Follow the vendor instructions.

3. Download the following file for the Apache version that you installed:

   `mod_jk.so`

   We recommend that you download the latest version.

4. Copy the mod_jk.so file to the following folder:

   `apache_install_dir``\modules`

5. Navigate to the following folder on the CA Process Automation installation media:

   `install_dir``\DVD1\ApacheConfTemplates`

6. Extract the following files from the appropriate zip folder:

   `mod-jk.conf`

   `uriworkermap.properties`

   `workers.properties`

   `httpd VIRTUALHOST_EXAMPLE FILE`

   > **Note:** The extracted httpd file contains text you can cut and paste into the Apache httpd file when you configure secure communications. The required text is also in the documentation.

7. Copy the extracted files to the following folder:

   `apache_install_dir``\conf`

Note: If you do not have an Apache 2.2 load balancer to dedicate, merge the configuration information in the example template properties and Conf files into your existing files. As a precaution, back up your files before you modify them.

Configure Basic Communication

You can configure a load balancer for basic communication with the nodes of the Domain Orchestrator or other Orchestrator.

Follow these steps:

1. Install a load balancer and prepare configuration templates (see page 35).
2. Navigate to the following folder that contains worker.properties and mod-jk.conf.

   ```
   apache_install_dir\conf
   ```

3. Open the workers.properties file.
4. If this is the first node you are adding, go to the section beginning with the comment, Define node1. Locate the following line:

   ```
   worker.node1.host=<Enter node1 hostname here>
   ```

5. Replace the *Enter node1 hostname here* placeholder for worker.node1.host to the actual value.

   Note: The value can be the IP address, the FQDN, or the DNS alias that resolves to the host where you are installing the initial Domain Orchestrator node. This value is the same value that is used for “Server Host” when installing the Domain Orchestrator.

6. Save the workers file.
7. Close the file.

Configure Secure Communication

You can configure a load balancer for secure communication. CA default locations are documented in the openssl file in the conf folder of the Apache installation location.

In the following steps, your certificate location is designated as *certloc*.

Follow these steps:

1. Install a load balancer and prepare configuration templates (see page 35).
2. Configure basic communication (see page 37).

3. Create or obtain a certificate file and private key file with a “Common Name” matching the “ServerName” in httpd.conf (without the port).

   One series of commands to do this step follows. These commands use the *openssl utility* that is provided with the Apache load balancer. Additional options control certificate expiration, file names, and algorithms. You can reference the vendor-provided documentation if your site has special requirements.

   a. Open a command prompt

   b. Change directories to the Apache bin folder.

      ```
      cd apache_install_location/bin
      ```

   c. Create a Certificate Signing Request file (csr) and PEM files. Type the following command, where “mypamserver” is a name of your choice.

      ```
      openssl req -config ../conf/openssl.cnf -new -out
      mypamserver.csr
      ```

      You are prompted for the pass phrase for the PEM file, and other identifying information.

      - For most identifying information (Country Name, State or Province Name, Locality Name, Organization Name, Organization Unit Name), you can accept the default value. To leave a field blank, enter a dot (.).
      - When the Common Name prompt appears, enter as the value the hostname portion of “ServerName” in *apache_install_location/*conf /httpd.conf.

        For example, if “ServerName” in httpd.conf has the value myhost.mycompany.com:80, specify **myhost.mycompany.com** as the “Common Name”.
      - Optional fields include: Email address, dir, a challenge password, and an optional company name.

      On completion, files *mypamserver.csr* and *privkey.pem* are created in the current directory.

   d. Create your private RSA key. When prompted, enter a passphrase for privkey.pem.

      ```
      openssl rsa -in privkey.pem -out mypamserver.key
      ```

   e. Create your certificate.

      ```
      openssl x509 -in mypamserver.csr -out mypamserver.cert -req
      -signkey mypamserver.key
      ```

4. Close the command prompt and open Windows Explorer to copy and delete generated files:

   a. Select or create a folder to hold your certificate and private key files, your *certloc* folder).

   b. Open the *apache_install_dir*\bin folder, where the CERT and KEY files were generated.

   c. Drag and drop (move) *mypamserver*.cert and *mypamserver*.key to *certloc*.

   d. Delete the intermediate files created in the bin folder. Other intermediate files include mypamserver.CSR, privkey.PEM, and .RND.

5. Back up your files.

6. Using a text editor, modify the httpd text file, *apache_install_location*\conf\httpd.conf, as follows:

   a. Uncomment the following lines:

      ```
      LoadModule rewrite_module modules/mod_rewrite.so
      ```

      ```
      LoadModule ssl_module modules/mod_ssl.so
      ```

      ```
      Include conf/extra/httpd-ssl.conf
      ```

   b. Add the following lines at the end of “httpd.conf”. You can copy and paste the text from the extracted httpd VIRTUALHOST_EXAMPLE file.

      ```
      <VirtualHost *:80>
      JkMountFile conf/uriworkermap.properties
      RewriteEngine On
      RewriteCond %{HTTPS} off
      RewriteCond
      http://%{HTTP_HOST}%{REQUEST_URI}!^http://.*c2orepository*|
      MirroringRequestProcessor*|mirroringrepositry*|StartAgent*|
      genericNoSecurity*|soapAttachment*
      RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
      </VirtualHost>
      #Load balancing module
      Include conf/mod-jk.conf
      ```

      Note: The second RewriteCond is wrapped across many lines. You can copy and paste this section from the httpd.virtualhost_example found in the SecureDomainConfig_Template.zip.

   c. Save modified httpd.conf file and exit editor.

7. Back up your files.

8. Using a text editor, modify *apache_install_location/*conf/extra/httpd-ssl.txt configuration file as follows:

   a. Uncomment (If commented): “Listen 443”

   b. Change SSLCertificateFile location to .../*certloc/mypamserver.*cert, for example:

   ```
   SSLCertificateFile "C:/certloc/mypamserver.cert"
   ```

   c. Change SSLCertificateKeyFile location to .../*certloc/mypamserver.*key, for example:

   ```
   SSLCertificateKeyFile "C:/certloc/mypamserver.key"
   ```

   d. Add the following lines as the last two lines within the <VirtualHost> element, that is, on lines preceding </VirtualHost>.

   ```
   SSLOptions +StdEnvVars +ExportCertData
   JkMountFile conf/uriworkermap.properties
   ```

   e. Save modified httpd.conf-ssl file and exit the editor.

9. Restart the Apache service. From the Start menu, click Programs, Apache HTTP Server 2.2, Control Apache Server, Restart.

   The changes take effect.

F5 Load Balancer Prerequisites

If you have an F5 load balancer, you can use it to balance operator requests or web services requests to CA Process Automation clustered nodes. The F5 functionality is likely used for network nodes, pools, virtual machines, and iRules that are not used for CA Process Automation.

To prepare for F5 load balancing with CA Process Automation, the nodes must be defined up front. This can be done before installing the Orchestrator node. It can be done from your plan of how you intend to build out the CA Process Automation system.

In summary, prerequisite to using F5 for load balancing an Orchestrator cluster, you must have the following on hand:

- F5 load balancer technology.
- Identification of servers or virtual servers where Orchestrator nodes will be deployed.
- A virtual server.
- Credentials to log in to the F5 interface.

You must configure the following F5 elements so that they function with CA Process Automation.

1. Create an F5 node for each cluster node (see page 42).

   For CA Process Automation, a node is any server on which an Orchestrator or Orchestrator node is installed (or could be installed in the future).

2. Create an F5 pool for each CA Process Automation cluster (see page 43).

   For CA Process Automation, each pool includes Orchestrators belonging to the same cluster.

3. Create am F5 iRule for CA Process Automation (see page 44).

   For CA Process Automation, an iRule is code that routes CA Process Automation operator requests that target the touchpoint of a clustered Orchestrator. iRules specify how to determine the destination node. We supply the iRule; you set the variables.

4. Create an F5 virtual server for CA Process Automation (see page 46).

Create an F5 Node for Each Cluster Node

Rather than configuring cluster nodes after they are present in CA Process Automation, you configure the nodes that you expect to add to any clustered Orchestrator up front.

Follow these steps:

1. Log in to F5.
2. Select the Main tab, click Local Traffic, and then click Nodes.

   The Node List displays the following details for each network node that has been defined to F5: the status, the IP address, the partition, and the host name.
3. Click Create.

   The New Node page appears.
4. Complete the General Properties section.

   Address

   Specifies the IP address of the new node.

   Name

   Specifies the host name of the associated IP address.
5. Complete the Configuration section.

   Health Monitors

   Specifies the health monitor for this node. If it is not configured, select None.

   Default: Node Default

   Ratio

   Specifies a weighted value to assign to the node. If the nodes that belong to the same cluster all have the same capacity, enter 1 as the Ratio value for each node.

   Connection Limit

   Specifies the maximum number of connections that this node can handle.
6. Click Finished.

   The added node is displayed in the Node List.

Create an F5 Pool for Each CA Process Automation Cluster

Create an F5 pool for each CA Process Automation cluster. To each F5 pool that you create, add the nodes that belong to the associated cluster.

Follow these steps:

1. Log in to F5.
2. Select the Main tab, click Local Traffic, and then click Pools.

   The Pool List is empty if you are setting up pools for the first time. The Pool List displays the following details for each pool: the status, the pool name, the partition, and the number of members in the pool.
3. Click Create.

   The New Pool page appears.
4. Complete the Configuration section.
   a. Select Basic from the drop-down list.
   b. Enter a name for the new pool.
   c. From the available health monitors, select http and move it to the active list.
5. Select Round Robin from the Load Balancing Method drop-down list.
6. Select Disabled from the Priority Group Activation drop-down list.
7. Add each node to the new F5 pool as follows:
   a. Select Node List because you are adding a node that is defined.
   b. Select the IP address (host name) from the Address drop-down list that identifies the node to add to this F5 pool.
   c. Type **8080** for Service port.
   d. Click Add.

   The details that you added for this node appear in the New Members list.
8. Click Finished.

   The new pool is added to the F5 Pool List.

Create an F5 iRule for CA Process Automation

You can create an F5 iRule for CA Process Automation. An iRule definition is provided for you. For each iRule, copy the provided definition into the Description text box and set the variables, *MyPool*, *PrimaryIP*, and *PrimaryPort* to values specific to this iRule.

Note: An iRule is equivalent to uriworkermap.properties in apache.

Follow these steps:

1. Log in to F5.
2. Select the Main tab, click Local Traffic, and then click iRules.

   The iRules List is empty if you are setting up iRules for the first time. The iRules List displays the following details for each iRule: the iRule name and the partition.
3. Click Create.

   The New iRule page appears.
4. Complete the Properties section.

   Name

   Specifies the iRule name.

   Definition

   Specifies the iRule definition. Copy the text from The iRule Definition (see page 45) into this text box.

   Note: The programming language that is used for iRules is Tcl, Tool Command Language.

   Extend Text Area

   Specifies whether to extend the text area of the Definition text box to its maximum size.

   Selected - Extends text area to its maximum size.

   Cleared - Presents text area in a size that is less than maximum.

   Wrap Text

   Specifies whether to wrap the text to fit in the Definition text box rather than display a horizontal scroll bar.

   Selected - Wraps text that extends beyond the viewable portion of the Definition text box, excluding a horizontal scroll.

   Cleared - Presents text as entered, with a horizontal scroll bar if needed.
5. Click Finished.

   The iRule you enter appears in the iRule List.

The iRule Definition

Type the following definition in the Definition text box for your new iRule. Set the variables, *MyPool*, *PrimaryIP*, and *PrimaryPort* to values specific to the current pool. The PrimaryIP and PrimaryPort can refer to the IP address and port of the Domain Orchestrator, if clustered. These variables can also identify an additional Orchestrator, one not added as a cluster node.

```
when HTTP_REQUEST {
set PAMPOOL "[MyPool]"
set PRIMARY "[PrimaryIP]"
set PRIMPORT "[PrimaryPort]"
   switch -glob [HTTP::uri] {
          "/jmx-console*" { pool $PAMPOOL }
          "/web-console*" { pool $PAMPOOL }
          "/itpam*" { pool $PAMPOOL }
          "/c2orepository/oasisHelp*" { pool $PAMPOOL }
          "/c2orepository/htmlFile/aboutUs/*" { pool $PAMPOOL }
          "/c2orepository/htmlFile/language/*" { pool $PAMPOOL }
          "/itpam/ServerConfigurationRequestServlet" { pool $PAMPOOL member
$PRIMARY $PRIMPORT }
          "/itpam/MirroringRequestProcessor*" { pool $PAMPOOL member $PRIMARY
$PRIMPORT }
          "/c2orepository/*" { pool $PAMPOOL }
          "/mirroringrepository*" { pool $PAMPOOL member $PRIMARY $PRIMPORT }
          "/itpam/StartAgent*" { pool $PAMPOOL member $PRIMARY $PRIMPORT }
          "/itpam/OasisPrimary" { pool $PAMPOOL member $PRIMARY $PRIMPORT }
          "/c2orepository/htmlFile/installation/*" { pool $PAMPOOL }
          "/itpam/ServerConfigurationRequestServlet" { pool $PAMPOOL member
$PRIMARY $PRIMPORT }
          "/itpam/AgentConfigurationRequestServlet" { pool $PAMPOOL }
          "/birt/*" { pool $PAMPOOL member $PRIMARY $PRIMPORT }
          "/itpam/JNLPRequestProcessor*" { pool $PAMPOOL }
          "/itpam/JNLPRequestProcessor/installation" { pool $PAMPOOL member
$PRIMARY $PRIMPORT }
          "/c2orepository/media*" { pool $PAMPOOL member $PRIMARY $PRIMPORT }
          "/c2orepository/thirdParty*" { pool $PAMPOOL member $PRIMARY $PRIMPORT }
          "/itpam/clientproxy/c2oresourceaction" { pool $PAMPOOL member $PRIMARY
$PRIMPORT }
          "/itpam/clientproxy/c2oreportaction" { pool $PAMPOOL member $PRIMARY
$PRIMPORT }
          default { pool $PAMPOOL }
   }
}
```

Create an F5 Virtual Server for CA Process Automation

You can create an F5 Virtual Server. Specify that a CA Process Automation pool is the default pool. Specify the iRule that you created for this pool. If the Domain Orchestrator is clustered, the pool for this cluster is a good choice for the default pool.

Follow these steps:

1. Log in to F5.
2. Select the Main tab, click Local Traffic, and then click Virtual Servers.

   The Virtual Servers List displays the following details for each Virtual Server: the status, the name, the partition, the destination IP address, the service port, the type, and an Edit link for Resources.
3. Click Create.

   The New Virtual Server page appears.
4. Complete the General Properties section.

   Name

   Specifies the name of the virtual server, for example, PAMLB.

   Destination Type

   Specifies Host for a single IP address.

   Destination Address

   Specifies the IP address of the Virtual Server, for example, 10.130.5.149.

   Service Port

   Specifies a port, for example, 80 for HTTP.

   State

   Specifies whether the virtual server is available for load balancing. Specify Enabled.
5. Complete the Configuration section. Accept all defaults, except for HTTP Profile.

   Type

   Specifies the type of virtual server. Standard is a virtual server that directs all traffic to the pool you defined as the default load balancing pool.

   Default: Standard

   HTTP Profile

   Specifies the HTTP profile for managing HTTP traffic. Select http.

6. Complete the Resources section.

   iRules

   Specifies the iRules to enable for this virtual server. Select the iRules script that you created for the Domain Orchestrator.

   Default Pool

   Specifies the name of the pool that the virtual server routes traffic to, unless the selected iRules script redirects traffic.

   Default Persistence Profile

   Specifies the persistence profile for this virtual server. For example, source_addr.

   Fallback Persistence Profile

   Specifies the persistence profile that this virtual server uses when the default persistence profile cannot be used. For example, dest_addr.

7. Click Finished.

Time Synchronization Prerequisites

It is recommended that you synchronize the Domain Orchestrator time with a standard external time server. This prepares the Domain Orchestrator for the time when a cluster node is added. A cluster node for any Orchestrator must have the exact same clock time as the primary node. Time synchronization is not handled by the load balancer.

More information:

Synchronize Time for a Cluster Node (see page 103)

Port Planning Prerequisites

Ports are configured during installation. When configuring network ports, accept defaults except when:

- The default port is used by another application on the host.
- A firewall restriction prevents communication on the default port.

Review the use of the following ports and plan for substitutions for any ports listed here that are in use in your network or on the applicable host. With the exception of the port for agents and for CA EEM, all other properties are stored in the OasisConfig.properties file in *install_dir*/server/c2o/.config. If a conflict occurs after installation, you can modify this file manually.

162 oasis.snmptrigger.service.port

1090 jboss.remoting.port

1098 jboss.rmi.port

1099 jboss.jndi.port

1100 jboss.ha.jndi.port

1101 jboss.ha.jndi.rmi.port

1102 jboss.mcast.jndi.autodiscovery.port

3306 oasis.database.dbport

3306 oasis.reporting.database.dbport

3306 oasis.runtime.database.port

3528 OAPort

3529 OASSLPort

3873 jboss.remoting.transport.Connector.port

4444 jboss.rmi.object.port

4445 jboss.ha.pooledinvoker.serverbind.port

4446 jboss.pooledinvoker.serverbind.port

4447 jboss.ha.rmi.object.port

4448 remoting.transport.connector.port

4457 jboss.service.binding.port

4712 jboss.tx.recovery.manager.port

4714 jboss.tx.manager.sock.pid.port

5445 jboss.jbm2.port

5446 jboss.hbm2.netty.ssl.port

5250 *default port for CA EEM*

7001 oasis.jxta.port

7003 *default port for agents*

7600 jboss.jgroups.tcp.tcp_port

7650 jboss.jgroups.tcp_sync.tcp_port

7900 jboss.messaging.datachanneltcpport

7901 jboss.messaging.controlchanneltcpport

8009 tomcat.connector.ajp.port

8080 tomcat.connector.http.port

8083 jboss.rmi.classloader.webservice.port

8093 jboss.uil.serverbind.port

8181 ucf.pax.web.http.port

8443 tomcat.secure.port

45566 jboss.mcast.ha.partition.port

45567 jboss.mcast.http.sessionreplication.port

61616 ucf.bus.port

61617 ucf.bus.http.port

Interactive Domain Orchestrator Installation

Installation of the CA Process Automation Domain Orchestrator depends on certain components being present. Therefore, installation of CA Process Automation is done in two major phases:

1. Installing the third-party software.
2. Installing the Domain Orchestrator.

Both steps must be performed whenever installing, reinstalling, or upgrading CA Process Automation.

Installation can be performed from physical media, from a copy that you make of the physical media or that you obtain though download.

You can exit the installation process at any time. If you cancel, a confirmation pop-up displays. If you confirm the cancelation, the installation steps you have taken are rolled back.

Subsequent installations require certain values that you configure during Domain Orchestrator installation. For example, certain passwords must be reentered during upgrade or installation or other Orchestrators. A simple way to retain a record of values you enter is to create a plan for passwords before you begin interactive installation. For example, record passwords for the following plus any database server specific passwords.

- CA Process Automation certificate.
- CA EEM certificate.
- Repository database.
- Reporting database.
- Runtime database.
- CA EEM administrator.

More information:

Unattended Domain Orchestrator Installation (see page 65)

Installing CA Process Automation in Embedded Mode

During the CA Process Automation Domain installation, you are asked to choose the type of installation to perform:

- Standard installation
- Embedded mode installation

  See Using an Embedded Mode CA Process Automation (see page 135).

If you choose embedded mode, you do not configure CA EEM and you do not provide any settings for an external database. You simply specify a few parameter values for Derby, such as port, host, and network mode.

After you install CA Process Automation in embedded mode, you can install with the regular installation. However, after you install CA Process Automation as the regular installation, you cannot override it with embedded mode.

Install the Third Party Software

You can install the third party software.

Follow these steps:

1. Insert DVD1 of the CA Process Automation installation media into a drive or browse to the location where the installation files were copied.
2. Run the installation program appropriate to your platform and media:

   Windows

   - DVD1: Domain_Installer_windows.bat
   - Copied location:
     - Third_Party_Installer_Windows_32.exe
     - Third_Party_Installer_Windows_64.exe (Required If only a 64-bit JDK is installed.)

   HP-UNIX

   - DVD1: Domain_Installer_hpux.sh
   - Copied location: Third_Party_Installer_hpux.sh

   Linux or UNIX

   - DVD1: Domain_Installer_unix.sh
   - Copied location: Third_Party_Installer_Unix.sh
3. Select the preferred language from the Language Selection dialog.

   This sets the default language. Regardless of the language selected, CA Process Automation is installed with support for all available localizations.

   The Welcome to the CA Process Automation 3rd Party Installer Setup Wizard appears.
4. Click Next to begin installation of third party components.
5. Read the license agreement. To accept, select I accept the terms of the License Agreement and click Next.
6. Click Next to install the components in the default destination directory. Or, browse to a different directory and then, click Next.

   The installer creates the folder automatically if it does not exist. A minimum of 8GB disk space is required.

   Important! Ensure that the CA Process Automation folder structure including installation location does not exceed 255 characters. CA Technologies recommends keeping the installation location to 64 characters or less.

   The list of prerequisites appears. Prerequisites for the Domain Orchestrator include JBoss Installation, Hibernate Installation, and JDBC Jar Installation.

7. Click Next.

   Monitor the installation of JBoss and third party components.

   The JDBC Jars Installation appears.

8. Select one or more database server applications to use for internal access to CA Process Automation databases and specify the path to the appropriate JDBC driver jar file. Then, click Next.

   - MySQL - Browse to a JDBC driver jar file you have previously downloaded for MySQL. For example:

     `...`*`your_dir`*`\mysql-connector-java-5.1.19-bin.jar`

   - MS SQL - Accept the default path to the JDBC jar file on DVD1 installation disk. For example:

     `...\DVD1\drivers\sqljdbc.jar`

     (Optionally, you can browse to a different JDBC jar file.)

   - Oracle - Accept the default path to the JDBC jar file on DVD1 installation disk. For example:

     `...DVD1\drivers\ojdbc14.jar`

     (Optionally, you can browse to a different JDBC jar file.)

   Note: You must specify at least one JDBC driver. Specifying multiple JDBC drivers for internal communication is typically not necessary. During the Domain Installation, you can install additional JDBC drivers for use by other Orchestrators, or Agents with the Database operators (formerly the JDBC Module).

9. When the Completing the CA Process Setup Wizard displays, insert the CA Process Automation installation DVD2 or browse to the directory that contains the files from the DVD2 installation media. Then, click Finish.

   The Third Party Installer passes control to the CA Process Automation Domain Orchestrator installer.   There may be a short interval where the UI for the Third Party Installer will have closed and the UI for the CA Process Automation Domain install has not yet appeared. This is normal.

Install the Domain Orchestrator

This section applies to installing a standalone Domain Orchestrator or the first node of a clustered Domain Orchestrator.

After installing third party components, the installer will copy the CA Process Automation installer files to the host machine and start the Domain Orchestrator installer.

Follow these steps:

1. On the Welcome page, click Next.
2. Accept the license agreement, and click Next.
3. Verify that the displayed path is the path to the Java Home Directory. If it is not, click Browse, navigate to the correct location and select the Java Development Kit (JDK) to use. For example: C:\Program Files\Java\jdk1.7.0. Click Next.

   The JDK is validated.
4. Monitor the progress as files are copied.

   The CA Process Automation Domain Configuration Screen appears.
5. If you want to configure CA Process Automation for use with CA SiteMinder and all SiteMinder Prerequisites are met, enter the SSO information:

   Configure Single Sign-on (SSO)

   > Select this check box to configure CA SiteMinder with the Domain Orchestrator.
   >
   > Ensure that the CA SiteMinder WebAgent is configured with the same Apache Load Balancer that you plan to use for CA Process Automation.

   SSO Authentication Type

   > Specifies the authentication type when CA SiteMinder is configured. Select Header as the authentication type.
   >
   > The authentication type determines how CA Process Automation is informed of the User ID when a user is logged in through CA SiteMinder. Users can select the default values already populated in this list.

SSO Authentication Parameter

Specifies the name of the authentication parameter when CA SiteMinder is configured.

Select the default values already populated in this list, or enter new values depending on your SiteMinder configuration.

- Select sm_user as the SSO Authentication Parameter for IIS.
- Select SM_User as the SSO Authentication Parameter for Apache.

Type of Server

Keep as "New Orchestrator".

6. If you are not using an Apache load balancer, go to Step 7. If you plan to configure a clustered Domain Orchestrator, or if you are configuring for use with SiteMinder, read the directions for the section and then complete this page. Then click Next.

Configure Load Balancer

Specifies whether to install the Domain Orchestrator with the potential for clustering.

Selected: Install the Domain Orchestrator with the potential for clustering. This option assumes you have completed Apache Load Balancer Prerequisites (see page 34).

Cleared: Install the Domain Orchestrator with no potential for clustering.

Load Balancer Worker Node (Apache)

Specifies the name of this node. Since the Domain Orchestrator is the first node in the cluster, this is **node1**.

If your load balancer is Apache, your entry must match the name you specified for worker.node1.host in the Apache workers.properties file in *apache_install_dir*\conf. For example:

```
worker.node1.host=DomainOrchestratorHost.mycompany.com
```

Public Host Name

Specifies the public host name. For example:

loadbalancerhost.mycompany.com

- If Configure Single Sign-on (SSO) is selected, this field must contain the FQDN of the IIS/Apache on which the CA SiteMinder WebAgent is configured.
- If Load Balancer is selected without the Configure Single Sign-on (SSO) option, then this field must contain the FQDN of the load balancer.

Public Host Port Number

If Support Secure Communication is cleared, specifies the HTTP port for IIS/Apache, the Public Host.

Default

80

If you change this value during the Load Balancer installation and configuration, then update this value accordingly. This port and the Public Host Name value are used to browse to CA Process Automation. For example:

`http://`*`public-host-name`*`:80/itpam`

Public Host Secure Port

If Support Secure Communication is selected, specifies the HTTPS port for IIS/Apache, the Public Host.

Default

443

This port is part of the URL used to access CA Process Automation Web services. This port and the Public Host Name value is used to browse to CA Process Automation. For example:

`https://`*`public-host-name`*`:443/itpam`

Support Secure Communication

Specifies whether to use of HTTPS for secure communication.

Selected

Indicates that the IIS/Apache, the Public Host, communicates using HTTPS.

Note: If you performed the "Configure Secure Communication" steps for Apache, select this option.

Cleared

Indicates that the IIS/Apache, the Public Host, communicates using HTTP.

7. Type your company name, and click Next.

   Your entry appears in Help -> About as the string following “This Product is licensed to:”.

8. Type a certificate password and type it again as confirmation

   Certificate Password

   Creates the password that controls access to the keys used to encrypt passwords and other critical data. You must enter this same password when installing any other Orchestrator or when adding cluster nodes to an Orchestrator. The password is specific to a single CA Process Automation Domain.

   Confirm Certificate Password

   Confirms the password by matching your entry with the preceding entry.

   Important! Before you click Next, record your entry for Certificate Password in a secure location for later reference.

9. (Windows only) Specify the following Start Menu preferences. Then click Next.

   [Start menu folder name]

   Accept the default or type the name of the Start menu folder for CA Process Automation if Do not create a Start menu folder is Cleared.

   Default

   CA Process Automation 4.0

   Create shortcuts for all users

   Specifies whether the specified short menu folder name is displayed for all users who log on to the server with the CA Process Automation Domain Orchestrator.

   Selected - Display shortcuts.

   Cleared - Do not display shortcuts.

   Do not create a Start menu folder

   Specifies whether to create an entry for CA Process Automation in the Start menu.

   Selected - Create an entry in the Start menu for CA Process Automation.

   Cleared - Do not create a Start menu entry for CA Process Automation.

10. Enter the General Properties for the Domain Orchestrator.

    The following values define how the Domain Orchestrator communicates with other CA Process Automation components and applications.

    Server Host

    Specifies the host name or IP address of the host system on which the Domain Orchestrator is deployed, or a DNS Alias which will resolve to the host system.

    Display Name

    Specifies the Domain Orchestrator name displayed in the CA Process Automation Configuration browser.

    - If you do not configure a load balancer, the Display Name is the same as the Server Host name.
    - If you configure a load balancer, the Display Name is the FQDN of the server where the load balancer is installed.

    Server Port

    Specifies the port that the Domain Orchestrator uses to communicate with other Orchestrators and agents.

    Default: 7001

    HTTP Port

    When Support Secure Communication is cleared, specifies the HTTP port used for the Web Server.

    Default: 8080

    Note: This port is part of the URL used to access CA Process Automation Web services and the CA Process Automation login screen.

    JNDI Port

    Specifies the Java naming server port used by the Web Server.

    Default: 1099

    Note: This port must not be accessed from outside of this host system.

    RMI Port

    Specifies the RMI port used by the Web Server.

    Default: 1098

    Note: This port must not be accessed from outside of this host system.

SNMP Port

Specifies the SNMP trap listener port for CA Process Automation.

Default: 162

HTTPS port

When Support Secure Communication is selected, this specifies the port to be used in the URL used to access CA Process Automation Web services, and the URL used to access the browser-based CA Process Automation UI.

Default: 8443

Note: You must check “Support Secure Communication” to enable input to this field.

Support Secure Communication

Specifies whether communication to CA Process Automation is secure, as opposed to the standard basic communication. This value controls whether the HTTP Port or the HTTPS Port is enabled.

Selected - Use the HTTPS protocol for communication.

Cleared - Do not use the HTTPS protocol for communication. User HTTP instead.

Install as Windows service

Specifies whether to install the Domain Orchestrator as a Windows Service. Selected is valid only when CA Process Automation is installed on a Windows server.

Selected - Install CA Process Automation as a Windows service.

Cleared - Do not install CA Process Automation as a Windows service.

Click Next to continue.

11. Accept the default path or browse to a temporary directory in which to execute scripts, and then click Next.

    This directory must be writable by all users.

12. Specify settings for PowerShell and click Next.

    Set Powershell Execution Policy

    Specifies whether to enable the use of PowerShell.

    Selected - Enable the use of PowerShell. This sets the execution policy of the PowerShell at the specified path to Remote Signed.

    Cleared - Do not enable the use of PowerShell.

    PowerShell Path

    The PowerShell path is auto-detected.

    Note: When you click Next, the installer validates that the provided PowerShell path is not empty.

13. Specify the CA EEM security settings. Then register CA Process Automation with CA EEM and test the CA EEM settings.

    FIPS compliant certificate

    Specifies whether to use a FIPS compliant certificate. Selecting this option is valid only if CA EEM was installed with FIPS Mode set to on.

    Selected - Use encryption algorithms that are compliant with FIPS when transferring data between CA Process Automation and CA EEM. A FIPS-compliant certificate is a pem certificate type that includes the Certificate Key File that is retrieved from CA EEM when you register CA Process Automation with CA EEM.

    Cleared - Use other encryption algorithms. Use the specified EEM Certificate File (PAM.p12 is the default) with the specified EEM Certificate password.

    EEM Server

    Specifies the FQDN of the CA EEM server that CA Process Automation uses to authenticate and authorize CA Process Automation users. You can specify a backup CA EEM server if you are configuring EEM for High Availability (HA). Use a comma as the delimiter between the server names.

    EEM Application Name

    Specifies the application name for CA Process Automation. Normally you can accept the default value. However if you are using the same CA EEM server with multiple CA Process Automation Domains, each must be given a unique application name.

    Default: Process Automation

    EEM Certificate File

    Specifies the Certificate File. You should generally accept the default value.

    Defaults:

    - PAM.p12 - if you cleared the FIPS-compliant certificate setting.
    - PAM.pem - if you selected the FIPS-compliant certificate setting.

Certificate Key File

During registration, a certificate key is provided if CA EEM is configured for FIPS mode.

EEM Certificate Password

Specifies the CA EEM Certificate password.

Register Application

Specifies the options for registering CA Process Automation.

Selected - Specifies to enable the Register button.

Cleared - Specifies to not enable the Register button.

Register

Click this button to begin the registration process.

The EEM Credentials popup window appears. Complete the following fields and then click OK

EEM Admin Username

Specifies the user name for the CA EEM Administrator. Type **EiamAdmin**.

Default: EiamAdmin

EEM Admin Password

Specifies the password for the EiamAdmin user account. If you installed CA EEM, enter the password you created for the EiamAdmin user. Otherwise, contact an individual who administers the existing CA EEM and obtain the password.

When the Application registered confirmation appears, click OK.

Test CA EEM Settings

Click this button to begin the CA EEM settings test. After you have observed the results, click OK. Then click Next.

Type **pamadmin** for Username. Type **pamadmin** for Password. Click OK

The Verify EEM setting screen displays the following:

Connect

Specifies if connection to the given CA EEM server can be established with the application name, certificate and certificate password provided in the CA EEM settings screen.

Limits: OK and NOT OK

Note: If the value evaluates to NOT OK, the following fields are not displayed.

User provided belongs to User Group

Specifies whether pamadmin belongs to the application user group (PAMUsers (earlier ITPAMUsers)).

Limits: OK and NOT OK

User is an Admin

Specifies whether the pamadmin belongs to the application admin group (PAMAdmins (earlier ITPAMAdmins)).

Limits: Yes and No

EEM Upgrade

Specifies whether the CA Process Automation application schema in the EEM server is upgraded. When the value is NOT OK, upgrade the instance.

Note: This field is displayed only when the value is NOT OK.

14. Enter the database settings for the Library database, designated here as Repository database. Click Test Database Settings to test connectivity from CA Process Automation to the specified database server using the specified database port and with the specified jar file. Click Create Database to gain access and create the Library database on the specified server with the specified Database Collation. Then, click Next.

Type of Database

Specifies the Database system type. Use the drop-down list to select one of the currently supported types.

Values: MySQL, MS SQL, Oracle

Note: We recommend that you select either MS SQL or Oracle if this installation is for production use. MySQL is an appropriate choice for a lightly loaded Domain Orchestrator. Embedded mode uses the Derby database.

User Name

Specifies a user name authorized to create and access the database on the database server. The account must have permissions to create the database on the server or ownership (dbo) for an existing database. For example:

- If you selected MS SQL, enter sa as the User Name.
- If you select MySQL, enter root as the User Name.

Password

Specifies the password for the user name account.

Database Server

Specifies the host name or IP address of the database server.

Database Port

Specifies the connection port configured on the database server. For MS SQL, the port is 1433. For MySQL, the port is 3306.

Repository Database

Specifies the name of the database to store Library objects and other data.

Each Orchestrator can have its own repository, or library, database. Or, you can share the library database across Orchestrators. Each database must have a unique name. Consider establishing a naming convention for your CA Process Automation databases with this initial installation.

Driver Jar

Specifies the JDBC driver jar file for specified database type. Defaults for Microsoft SQL Server and Oracle database servers are provided in the drivers folder in the DVD1 folder of the installation media.

Defaults:

SQL Server: sqljdbc

Oracle: ojdbc14

MySQL: Click Browse. Navigate to the jar file you downloaded, for example mysql-connector-java-5.1.18-bin.jar

Database Collation

For MS SQL and Oracle, specifies the rule set for sorting data, where case-sensitivity, accent marks, kana character types and character width can be part of the rule set. This field is a drop-down list. This field is not applicable to MySQL. We recommend that you accept the default value.

Default: SQL_Latin1_General_CP1_CI_AS

Test Database Settings

Lets you test whether the specified database settings result in a successful connection to the database server. If a message indicates that the databases are missing, close the dialog and click the Create Database button. Except for Oracle, databases required by the Orchestrator can be created during installation.

Create Database

If you specified MS SQL or MySQL, click this button to create the Repository Database.

Note: When using an Oracle database server, you already created the Repository database as part of the database server prerequisite tasks.

A message indicates that a database has been created with the name you provided.

15. Enter the Runtime Database information, either manually or by copying specifications from your entries for the Repository Database. Click Create Database if the Type of Database is MSSQL or MySQL. Click Test Database Settings. Then, click Next.

    The Runtime Database fields are similar to the Database Setting fields for the Repository (Library) Database except for two fields. Refer to the previous step for descriptions of other fields.

    copy from main repository

    > Specifies whether to copy library database settings to the runtime database settings screen.
    >
    > **Selected** - Copies the library database settings to this dialog.
    >
    > This option can save you time if you are using the same database server for both CA Process Automation databases. If you select this option, type the runtime database name in the Runtime Database field. Then click Test Database Settings. Then click Create Database.
    >
    > **Cleared** - Does not copy the library database settings to this dialog. This option is appropriate if you are using a different type of database for runtime data than you are using for library records.

    Runtime Database

    > Specifies the name of the database or schema in which runtime instances are stored. The database has to be unique across the Orchestrators, thus no two Orchestrators can point to the same runtime database. Enter a unique name, for example, PAM_Runtime.
    >
    > **Default:** pam
    >
    > **Important!** You cannot share Runtime across Orchestrators. Un-installing and re-installing the product restricts you to use the same Runtime database.

    Queues Database

    > Specifies the name of the database where pending requests and responses are stored. Enter a unique name, for example, PAM_Queues.

16. Enter the Reporting Database information, either manually or by copying specifications from your entries for the Repository Database. Click Test Database Settings and, if the Type of Database is MS SQL or MySQL, click Create Database. Then, click Next.

    The Reporting Database fields are similar to the Database Setting fields for the Repository (Library) Database except for two fields. Refer to Step 14 for descriptions of other fields.

    copy from main repository

    > Specifies whether to copy library database settings to the Reporting database settings screen.
    >
    > **Selected** - Copies the library database settings to this dialog.
    >
    > This option can save you time if you are using the same database server for both CA Process Automation databases. If you select this option, type the reporting database name in the Reporting Database field. Then click Test Database Settings. Then click Create Database.
    >
    > **Cleared** - Does not copy the library database settings to this dialog. This option is appropriate if you are using a different type of database for reporting data than you are using for library records.

    Reporting Database

    > Specifies the name of the reporting database that stores all the generated reports. Enter a unique name, for example, PAM_Reporting.

17. Select the additional jars, typically JDBC drivers that you want to include in the installation.

    By default the JDBC drivers uploaded in the Third Party Software installation are displayed and are unchecked. You can add additional jars using the Add Files button.

    You must place a check for every jar that you want deployed. Verify that you selected all of the drivers that you want to deploy for JDBC Operator usage on CA Process Automation agents and Orchestrators. You can add additional drivers using the Add Files button.

    It is not necessary to anticipate the needs of designers for JDBC drivers. A domain administrator can deploy JDBC drivers as they are needed.

    Note: See the *Content Administrator Guide* chapter "Manage User Resources" for details on adding and managing Orchestrator and agent resources, including JDBC jar files.

    Once you are satisfied with your selection of additional jars, click Next.

18. Monitor the installation progress. The installer copies and signs all CA Process Automation components. This may take a few minutes.

19. Click Finish to exit the installer.

    Installation of the Domain Orchestrator is complete.

See How to Start or Stop an Orchestrator for how to start your Domain Orchestrator. It is suggested that you verify the correct operation of this initial Orchestrator before proceeding with additional configuration.

Unattended Domain Orchestrator Installation

CA Process Automation provides the option to install the Domain Orchestrator silently, or unattended, through the use of a response file. The response file contains various predefined parameters for use during the installation process. Once you create a response file, you can edit and run the install script file to begin the installation.

An example response file has been provided in the root folder of DVD1. We recommend that a copy of this file is used as the base for your response file.

Create a Response File

The first step in performing a silent installation of CA Process Automation is to create a response file.

Notes about the response file:

- Do not change the variable names. They are used in the installation. Changing the name of a variable is equivalent to not defining a variable.
- When specifying folder locations, use forward slashes "/" as directory separators.
- Use the hash (#) character to comment out any variables that you do not want to use.
- See the installation logs for any errors:

  ```
  ${install_dir}/server/c2o/installation.log
  ```

To create a response file

1. Insert disc1 of the CA Process Automation installation media into a drive or browse to the location where the installation files were copied previously from the installation media.
2. Open the DVD1 folder.
3. Open response.varfile and provide the appropriate values.

   Note: Parameter descriptions are included in the file.
4. Save the file to the path with the silent install script file.

Run or Edit the Silent Install Script File

Once you create the response file, you can start the silent installation by doing one of the following options:

- Running the silent install script file, passing its included parameters through the command prompt (recommended for a single installation of CA Process Automation)
- Editing the install script file parameters, then running it (recommended when you are installing multiple orchestrators)

Install script files are:

Windows

Silent_Install_windows.bat

***NIX**

Silent_Install_hpux.sh

Silent_Install_unix.sh

Parameters include:

-VcertPassword

Specifies the password that is used to control access to the keys used to encrypt passwords.

-VeiamCertPass

Specifies the password for the CA EEM certificate. For example, pamadmin

-VeiamPassword

Specifies the password for the database that is used for automation objects. For example, pamadmin

-VdbPassword

Specifies the password for the database that is used for automation. For example, objectsroot

-VreportingDbPassword

Specifies the password for the reporting database. For example, root

-VruntimeDbPassword

Specifies the password for the database that is used during runtime. For example, root

-VeiamAdminPass

Specifies the password for the CA EEM administrator, where the username is EiamAdmin. For example, eiamadmin

Important! Password parameters, whether passed through the command line or stored in the install script file, are not encrypted.

Once the installation completes, you can start the Orchestrator.

Post-Installation Tasks for the Domain Orchestrator

Perform the post-installation tasks that are applicable.

- If you reinstalled (not upgraded) the Domain Orchestrator so you could set secure communication using HTTPS, see Reinstalling the Domain Orchestrator From HTTP to HTTPS Mode (see page 71).
- If you installed CA Process Automation for the first time:
  - Configure ports (see page 48).
  - Configure firewalls for bi-directional communication (see page 69).
- To use Databases operators to connect to databases using a different RDBMS than CA Process Automation uses, install drivers for Database operators (see page 69).

  To use Windows Authentication (integrated security) with JDBC for MSSQL Server, install drivers for Database operators (see page 69).
- If you installed the Domain Orchestrator on a server with the HP-UX operating system, perform additional configuration steps on HP-UX. (see page 70)
- Tasks such as deploying drivers for Database operators require that you restart the Domain Orchestrator.
  - See Stop the Orchestrator (see page 73).
  - See Start the Orchestrator (see page 74).
- Before you configure the first administrator in CA EEM, you can browse to CA Process Automation and log in as the default administrator.

  See Browse to CA Process Automation and Log In as Default Administrator (see page 72).

Configure Firewalls for Bi-directional Communication

You must configure firewalls to allow bi-directional communication. Bi-directional communication is needed between the following component pairs:

- The Domain Orchestrator and the database server used for the Library database.
- The Domain Orchestrator and the database server it uses for its Reporting database.
- The Domain Orchestrator and the database server it uses for its Runtime database.
- The Domain Orchestrator and CA EEM.
- Each Orchestrator and the database server used for the Library database.
- Each Orchestrator and the database server it uses for its Reporting database.
- Each Orchestrator and the database server it uses for its Runtime database.

If you use local firewalls on Orchestrator or Agent host machines, make sure that CA Process Automation executables can listen and connect bi-directionally through the firewall on each host. Some host-based firewall programs (such as Windows Firewall) allow exceptions for executables.

Install Drivers for Database Operators

CA Process Automation designers can use operators from the Database category (formerly the JDBC module) to connect to various Relational Database Management Systems (RDBMSs). When the connection is to a MySQL database, an Oracle database, or a Microsoft SQL Server database, the correct drivers are available. (Availability of all three drivers depends on your selection during the Domain Orchestrator installation.) When the connection is to a database from a different vendor, you can deploy the JDBC driver for Database operators for that database from the CA Process Automation Configuration tab. For example, if a designer wants to use the Database operators for Sybase, an administrator deploys the JDBC drivers for Sybase. An administrator can deploy JDBC drivers on Orchestrators or on hosts with CA Process Automation agents.

Note: See "How to Deploy JDBC Drivers for Database Operators (itpam--howtoinstalljdbcdrivers.html)" in the Manage User Resources chapter of the *Content Administrator Guide* for procedures.

Additional Configuration Steps on HP- UX

For Orchestrators running on HP-UX, CA Process Automation requires max_thread_proc to be set to a value of 3000 or higher. If this is set to a value lower than 3000, the OS will be configured with an insufficient number of system threads, and you may encounter the following error when running Processes:

```
java.lang.OutOfMemoryError: unable to create new native thread
```

To change the value for max_thread_proc, do the following:

1. Start the SAM utility.
2. Click Kernel Configuration > Configurable Parameters.
3. For each of the parameters in the table, perform this procedure:
   a. Highlight the parameter to change.
   b. Click Actions > Modify Configurable Parameter.
   c. Type the new value in the Formula/Value field.
   d. Click OK.

Interact with the Desktop Configuration

Orchestrators and Agents normally run as console services and do not need to interact with the desktop. If an Orchestrator or Agent must interact with the Windows desktop, the Orchestrator or Agent service must start by using either a user account or by using the Local System account with the Allow service to interact with the desktop option selected. This option is selected by default when an Orchestrator or Agent is installed. Alternatively, this service can be configured using the Services console under Windows Administrative Tools. The check box to allow this privilege is under the Log On tab of the Properties Window for the service.

Enable Secure Communications for Existing CA Process Automation

If you previously selected HTTP as the protocol over which the Domain Orchestrator communicates, you can begin communicating over the secure HTTPS protocol.

Follow these steps:

1. Reinstall the Domain Orchestrator in one of the following ways:
   - Interactive Domain Orchestrator Installation (see page 49). In Step 10 of the installation procedure, select Support Secure Communication.
   - Unattended Domain Orchestrator Installation (see page 65). Set the isSecure variable in the Response file as follows to enable secure (HTTPS) communications:
     ```
     isSecure=true
     ```
2. Restart agents.

   HTTPS is used for all the communication between agents and the Domain Orchestrator.
3. Verify that all agents are updated and restarted.
4. Verify that all process instances that are using existing SOAP attachments are complete.

   Note: Existing SOAP attachments are accessible over HTTP only.
5. Define firewall rules to block the HTTP communications.

Browse to CA Process Automation and Log In as Default Administrator

Many of the topics in this guide assume that you have access to the CA Process Automation UI. Tasks such as deploying drivers, installing additional Orchestrators, and adding nodes are initiated from the Configuration tab in CA Process Automation. Administrators typically log in to CA Process Automation with their own credentials to perform such tasks.

Note: For details on creating your own user account, see Chapter 1 "Getting Started with CA Process Automation and CA EEM in the *Content Administrator Guide*.

CA Process Automation availability requires the following conditions:

- CA EEM is running.
- The load balancer, if used, is running.
- The Domain Orchestrator service is started.

  See Start the Orchestrator (see page 74).

To perform tasks that require access to CA Process Automation before you have a CA Process Automation user account, you can log in to CA Process Automation with the default administrator credentials.

Follow these steps:

1. Launch the URL. In the following example, *server* refers to the server where a nonclustered Domain Orchestrator is installed. For a clustered Domain Orchestrator, *server* refers to the server with the load balancer.

   - For secure communication, use the following syntax:
     `https://`*`server`*`:`*`port`*`/itpam`

     Examples:
     ```
     https://domainOrchestrator_host:8443/itpam
     https://loadBalancer_host:443/itpam
     ```

   - For basic communication, use the following syntax:
     `http://`*`server`*`:`*`port`*`/itpam`

     Examples:
     ```
     http://domainOrchestrator_host:8080/itpam
     http://loadBalancer_host:80/itpam
     ```

   The CA Process Automation login page opens.

2. Enter **pamadmin** for Username. Enter **pamadmin** for Password.
3. Click Log In.

   CA Process Automation opens. The Home tab displays.

Stop the Orchestrator

Only administrators with administrator credentials on the server where the Orchestrator is installed can stop the Orchestrator.

Follow these steps:

1. Using Administrator credentials, log on to host where the target Orchestrator is installed.
2. If you logged in to a Windows host, you can stop the Orchestrator service from the Start menu, the Services window, or the command line. Do one of the following:
   - Select Programs, CA, CA Process Automation 4.0, and Stop Orchestrator Service from the Start menu.
   - Select Administrative Tools and Services from the Control Panel. Select the following service and click Stop:

     ```
     CA Process Automation Orchestrator (C:\Program Files\CA\PAM\server\c2o)
     ```
   - Open a command prompt and run the following script, where XX is either 32 or 64, depending on the system.

     ```
     install_dir\\server\c2o\bin\wrapper_XX\stopc2osvc.bat
     ```
3. If you logged in to a UNIX or Linux host, do the following:
   a. Change directories to ${PAM_HOME}/server/c2o/. For example, change directories to:

      ```
      /usr/local/CA/PAM/server/c2o
      ```

   b. Run the c2osvrd.sh script with the - stop option. That is, run:

      ```
      c2osvrd.sh stop
      ```

Start the Orchestrator

Only administrators with administrator credentials on the server where the Orchestrator is installed can restart the Orchestrator service.

Follow these steps:

1. Using Administrator credentials, log on to host where the target Orchestrator is installed.
2. If you logged in to a Windows host, you can restart the Orchestrator service from the Start menu, the Services window, or the command line. Do one of the following:
   - Select Programs, CA, CA Process Automation 4.0, and Start Orchestrator Service from the Start menu.
   - Select Administrative Tools and Services from the Control Panel. Select the following service and click Start:

     ```
     CA Process Automation Orchestrator (C:\Program Files\CA\PAM\server\c2o)
     ```

   - Open a command prompt and run the following script, where XX is either 32 or 64, depending on the system.

     ```
     install_dir\server\c2o\bin\wrapper_XX\startc2osvc.bat
     ```

3. If you logged in to a UNIX or Linux host, do the following:

   a. Change directories to ${PAM_HOME}/server/c2o/. For example, change directories to:

   ```
   /usr/local/CA/PAM/server/c2o
   ```

   b. Run the c2osvrd.sh script with the start option. That is, run:

   ```
   c2osvrd.sh start
   ```

Note: After starting the service for the Domain Orchestrator, start CA Process Automation.

Chapter 5: Upgrading to the Current Release

This section contains the following topics:

Upgrade Prerequisites

When you upgrade CA Process Automation:

- If Microsoft SQL Server is the database server used, take steps to make the database XA enabled.

  Note: See Prepare Microsoft SQL Server for CA Process Automation (see page 26) for details.

- If you previously used LDAP or Microsoft AD for authentication and authorization, install CA EEM. CA EEM is the directory server for CA Process Automation Version 04.0.00.and above. Take one of the following approaches:

  - Create user accounts in CA EEM for your CA Process Automation users. Assign each user to a default group: PAMAdmins (full rights), Designers, or Production Users. PAMUsers has limited rights.

  - Create user accounts. Create custom policies in CA EEM to simulate the authorizations you used with LDAP.

  - Configure CA EEM to use your current LDAP directory server or Microsoft Active Directory as an external user store. Existing user accounts are loaded into CA EEM as global users and used for authentication. While you cannot update the loaded data from CA EEM, you can assign default application groups or custom groups to global users.

  Note: See "How to Transition Roles Used in Active Directory to CA EEM" in the "Administer Advanced CA EEM Security" chapter in the *Content Administrator Guide*.

- For cluster upgrades: Apache settings have changed. Change the existing settings in Apache to match the new settings. See Prerequisites to Installing a Cluster Node for the Domain Orchestrator (see page 97).

- If you installed CA Process Automation using an invalid DNS host name containing restricted characters such as underscores, take corrective action. See Resolve Invalid Character in CA Process Automation DNS Name (see page 126).

- If you are upgrading from a CA IT Process Automation Manager (CA IT PAM) release, see:

  - Special Considerations for Upgrade from 3.0 SP1 or Earlier (see page 77).

  - Special Considerations for Upgrade from 2.2 SP1 or Earlier (see page 77).

  - Special Considerations for Upgrade from Earlier than 2.2 SP1 (see page 78).

Special Considerations for Upgrade from 3.0 SP1 or Earlier

When upgrading from CA IT Process Automation Manager version 3.0 SP1 or earlier, you will need available twice the disk space as is currently consumed by your CA IT PAM databases available as free space to your Database Server. Because of this, and to speed the upgrade process, it is strongly suggested that unnecessary archive records be purged prior to upgrading.

Special Considerations for Upgrade from 2.2 SP1 or Earlier

The following prerequisites to upgrade apply if you are upgrading to the current release from CA IT Process Automation Manager r2.2 SP1 and earlier. Prerequisites apply if your database servers for CA Process Automation databases are MySQL or Microsoft SQL Server.

MySQL (MYISAM table type)

If the CA IT PAM tables are of MYISAM table type, convert the table types to innoDB before you upgrade.

SQL Server

Delete the JMS_MESSAGE_TXOP_TXID index instances from the JMS_MESSAGES table for each Orchestrator. The procedure follows:

To delete the JMS_MESSAGES_TXOP_TXID index

1. Open the Services window from your Windows Control panel.
2. Right-click the Orchestrator service and click stop.

   Note: If your Orchestrator is clustered, shut down both the Primary and Secondary nodes.

3. Launch SQL Server Management studio, and log in as the CA Process Automation user.
4. Expand the database tables you are using for CA Process Automation and browse to the JMS_MESSAGES table.
5. Expand the indexes of the JMS_MESSAGES table.
6. Right-click the JMS_MESSAGES_TXOP_TXID index, and select Delete.

   The JMS_MESSAGES_TXOP_TXID index is deleted.

7. Right-click the Orchestrator service and click restart.

How Dates Are Saved

All dates are saved in the database in Coordinated Universal Time (UTC). UTC is an international locale-independent standard which closely corresponds to the older Greenwich Mean Time (GMT).

At upgrade from a release of CA IT PAM before r3.0, all dates that CA Process Automation stored in the database are automatically converted to UTC. Dates are converted to UTC from the local time zone of the CA Process Automation Domain Orchestrator server.

Special Considerations for Upgrade from Earlier than 2.2 SP1

Upgrading from a CA IT PAM release earlier than 2.2 SP1 requires an intermediate upgrade before upgrading to the current CA Process Automation release.

Prerequisites follow:

1. If you have CA IT PAM databases hosted on MySQL and tables are of MYISAM table type, convert the table types to innoDB.
2. If CA IT PAM was using a 1.5 version of the JDK, upgrade to the JDK 1.6 version.
3. Purge unnecessary archive records.
4. Upgrade your CA IT PAM release that is earlier than r2.2 SP1 to one of the following: CA IT PAM r2.2 SP1, CA IT PAM r3.0, or CA Process Automation r3.1.

Upgrade to JDK Version 1.6

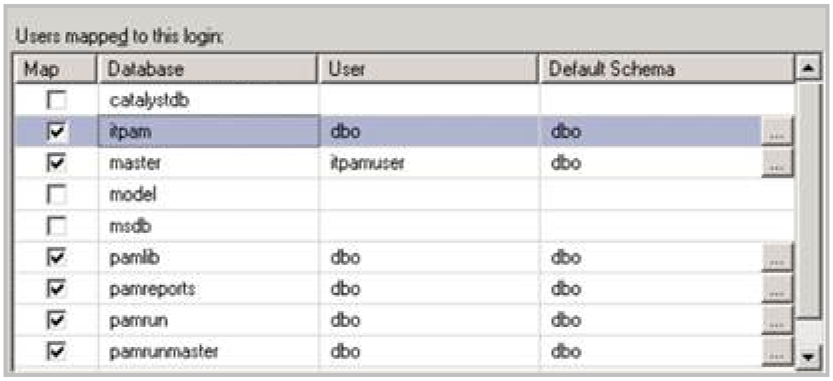
When upgrading CA Process Automation, verify that you are using the supported JDK version. You must upgrade if you are using a JDK version before 1.6. See Platform Support and Requirements for CA Process Automation Components (see page 18).

Enable XA Transaction Support in SQL Server Before Upgrade

The newer JBoss release 5.1.0 that the CA Process Automation server runs on requires support for XA transactions at the database level. Microsoft SQL Server must be configured to support and enable XA transactions. The directions assume that you previously used SQL Server for your CA Process Automation databases and that you configured **itpam** as your non-'sa' user.

Assumptions

Your SQL Server for a Domain Orchestrator houses three CA Process Automation databases: Library (pamlib), Runtime (pamrun), and Reporting (pamreports). (The Library database is the same thing as the Repository database.) The following example shows how each database is mapped to the dbo user and to the dbo default schema.

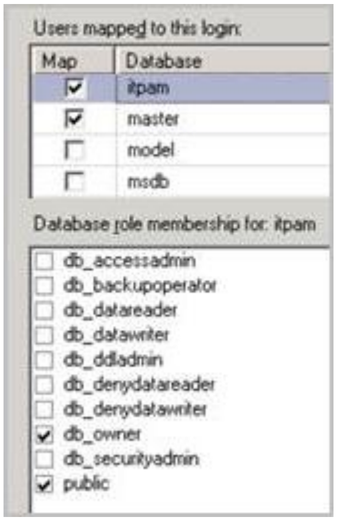


Users mapped to this login:

Map	Database	User	Default Schema
□	catalystdb		
☑	itpam	dbo	dbo
☑	master	itpamuser	dbo
□	model		
□	msdb		
☑	pamlib	dbo	dbo
☑	pamreports	dbo	dbo
☑	pamrun	dbo	dbo
☑	pamrunmaster	dbo	dbo

"itpamuser" is a dedicated non-SA user that has "dbo" access right to all schemas related to CA Process Automation and "db_owner" role and "SQLJDBCXAUser" for the "master" schema.

The database role membership for itpam includes db_owner and public, as shown on the following sample configuration:



Users mapped to this login:

Map	Database
☑	itpam
☑	master
□	model
□	msdb

Database role membership for: itpam

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ public

Procedure Summary

The high-level procedure follows:

- Have at hand the non-'sa' user name you created, for example, itpam. We refer to this user name as *pamuser*.
- Verify that *pamuser* is the owner (DBO) of each CA Process Automation database (or set DBO access)
- Verify that your existing JDBC driver that supports XA
- Copy required DLL library file to the SQL Binn folder and restart the SQL Server.
- Enable XA Transactions in Distributed Transaction Coordinator.
- Execute stored procedures to enable the transactions and define the new role.
- Map designated SQL server user to the “SqlJDBCXAUser” role.

Have at hand the non-'sa' database user name (*pamuser*) for CA Process Automation

If you do not know the non-'sa' database user, identify that user now.

1. Log in to the server where you installed the Domain Orchestrator.
2. Navigate to:

   `install_dir\c2o\.config`

3. Open the OasisConfig properties file in an editor.
4. Find the following string:

   `oasis.database.username=`

   The value for this parameter is the CA Process Automation database user. We refer to that user as *pamuser. Yo*ur name for this user can be different.

Verify that *pamuser* is the owner (DBO) of each CA Process Automation database in each SQL Server

If the user who created the database schema specified a user name in the "Owner" field, a DBO (database owner) association was created. Example user names include itpamuser, pamuser, and pamxauser. Verify that a DBO association with a user name was created. If the DBO was not created, create the association now.

1. Open Microsoft SQL Server Management Studio as user ‘sa’.
2. Review the properties of pamuser. Verify that the *pamuser* has DBO access to the following CA Process Automation databases: Repository database, Reporting database, Runtime database.
3. If *pamuser* does not have DBO access:
   - Select the CA Process Automation Repository database. Set *pamuser* as DBO. Save the setting.
   - Select the CA Process Automation Runtime database. Set *pamuser* as DBO. Save the setting.
   - Select the CA Process Automation Reporting database. Set *pamuser* as DBO. Save the setting.

Verify that your existing JDBC driver supports XA

The following JDBC drivers support XA transactions:

- Microsoft JDBC Driver 3.0 for SQL Server (sqljdbc.jar)
- Microsoft JDBC Driver 4.0 for SQL Server (sqljdbc4.jar)

Verify that the JDBC driver already installed supports XA transactions. If not, get the required JDBC driver from the path of the CA Process Automation installation media:

```
DVD1\thirdparty\mssql\sqljdbc_3.0\enu
```

Copy required SQLJDBC XA DLL library file to the SQL Binn folder and restart SQL server

1. Navigate to the appropriate xa directory:

   `DVD1\thirdparty\mssql\sqljdbc_3.0\enu\xa\x64`

   `DVD1\thirdparty\mssql\sqljdbc_3.0\enu\xa\x86`

   This directory contains the sqljdbc_xa.dll file.

2. Copy sqljdbc_xa.dll to the BINN folder on each SQL Server where a CA Process Automation database is installed, for example:

   `mssql_install_dir\MSSQL10.MSSQLSERVER\MSSQL\Binn`

   `mssql_install_dir\MSSQL.1\MSSQL\Binn`

   Tip: To identify the path to the BINN folder for the SQL Server being used:

   1. Run services.msc to open Services (Local)
   2. Scroll to SQL Server (MSSQLServer)
   3. Right-click and select Properties
   4. On the General tab, find the Path to executable.
   5. Copy the path into a text file. Use that path up to Binn folder as the destination BINN folder.

3. Restart the SQL Server.

   The SQLJDBC XA DLL installation script is loaded.

Enable XA Transactions in Distributed Transaction Coordinator

- If the SQL Server is using Windows 2008:
  1. From the Start menu, select Administrative Tools, Component Services.
  2. Expand Component Services, Computers, My Computer, and Distributed Transaction Coordinator.
  3. Right-click Local DTC and select Properties.
  4. Select the Security tab and select Enable XA Transactions.
  5. Click Apply, click OK. Close Component Services.
- If the SQL Server is using 2003
  1. Navigate to Administrative Tools, Component Services.
  2. Right-click My Computer and select Properties.
  3. Click the MSDTC tab.
  4. Click the Security Configuration button under Transaction Configuration.
  5. In the Security Configuration window, select Enable XA Transactions.
  6. Click Apply, click OK. Close Component Services.

Execute the xa_install.sql stored procedure to enable the XA transactions

1. Open Microsoft SQL Server Management Studio as the ‘sa’ user.
2. Select File, Open, File and then browse to the xa_install.sql script. For example, browse to:

   ```
   C:\temp\sqljdbc_3.0\enu\xa\xa_install.sql
   ```

3. Click Execute

   The source script, xa_install.sql, is executed as an extended stored procedure in SQL Server.

4. Ignore messages on permissions on xp_sqljdbc_xa_init.

Map the designated SQL Server user to the “SqlJDBCXAUser” role.

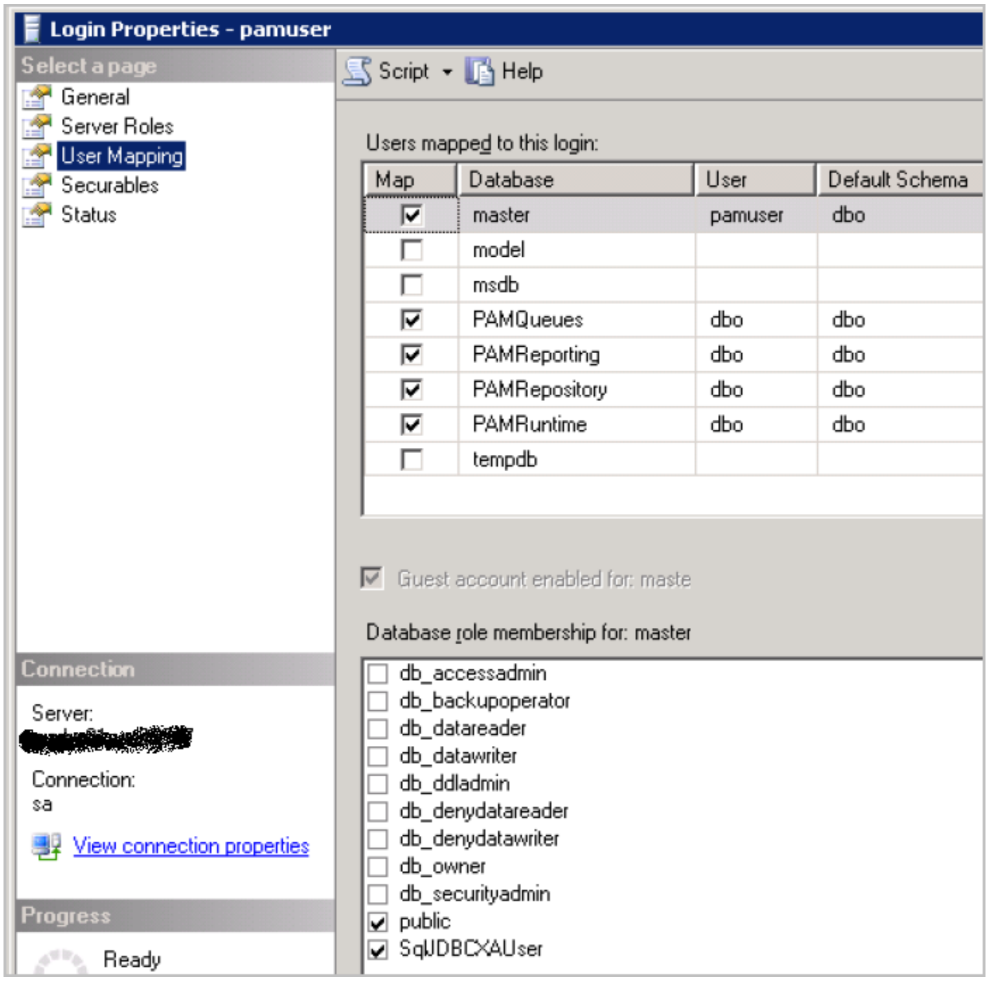
To grant permissions to *pamuser* to participate in distributed transactions with the JDBC driver, add *pamuser* to the SqlJDBCXAUser role. The SqlJDBCXAUser role in the master database grants access to the SQL JDBC extended stored procedures that are stored in the master database. First grant *pamuser* access to master, and then grant *pamuser* access to the SqlJDBCXAUser role while you are logged in to the master database.

1. With the extended stored procedures loaded, execute the following lines. For 'pamuser', substitute the value you located in in the OasisConfig.properties file for the oasis.database.username parameter.

   ```
   USE master

   GO

   EXEC sp_grantdbaccess 'pamuser', 'pamuser'

   GO

   EXEC sp_addrolemember [SqlJDBCXAUser],'pamuser'
   ```

2. Ignore the message that this user exists in the current database.

3. Verify that the SqlJDBCXAUser role is selected for the master database, where the master database user is *pamuser.*



Users mapped to this login:

Map	Database	User	Default Schema
☑	master	pamuser	dbo
□	model		
□	msdb		
☑	PAMQueues	dbo	dbo
☑	PAMReporting	dbo	dbo
☑	PAMRepository	dbo	dbo
☑	PAMRuntime	dbo	dbo
□	tempdb		

☑ Guest account enabled for: maste

Database role membership for: master

- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- □ db_owner
- □ db_securityadmin
- ☑ public
- ☑ SqlJDBCXAUser

Server:
[redacted]

Connection:
sa

4. Restart the SQL Server.

Browse to CA Process Automation and Log In

Browse to CA Process Automation. Enter either the fully qualified domain name (FQDN) or the IP address of the correct server.

Follow these steps:

1. Launch the URL where *server* refers to the server where the Domain Orchestrator is installed, if unclustered. For a clustered Domain Orchestrator, *server* refers to the server with the load balancer.

   - For secure communication, use the following syntax:
     `https://`*`server`*`:`*`port`*`/itpam`

     Examples:

     ```
     https://domainOrchestrator_host:8443/itpam
     https://loadBalancer_host:443/itpam
     ```

   - For basic communication, use the following syntax:
     `http://`*`server`*`:`*`port`*`/itpam`

     Examples:

     ```
     http://domainOrchestrator_host:8080/itpam
     http://loadBalancer_host:80/itpam
     ```

   The CA Process Automation login page opens.

2. Enter the user ID and password from the default administrator account or from your user account.

3. Click Log In.

   CA Process Automation opens. The Home tab displays.

Upgrade to CA Process Automation Service Pack 04.0.01

You can upgrade directly to CA Process Automation Service Pack 04.0.01 from CA IT PAM r2.2 SP1 or later. If you use CA EEM as your directory server, use the installer to perform the upgrade. Using the installer lets you retain existing user accounts and policies and maintain the registered name. Take the following steps so that CA EEM can authenticate and authorize CA Process Automation users who have CA EEM user accounts:

- Provide the *same* Application name to retain the old policies.
- Select Register to upgrade the CA EEM Application for CA Process Automation Service Pack 04.0.01.

Note: After upgrade, the default users and groups are retained in CA EEM, assuming that you provide the same application name. That is, ITPAMAdmins, ITPAMUsers, itpamadmin, and itpamuser accounts are retained if you provide the same application name and select Register.

You can upgrade to CA Process Automation Service Pack 04.0.01.

Follow these steps:

1. Reinstall the Domain Orchestrator in the same location where you installed the earlier version.

   Refer to the installation steps in Domain Orchestrator Installation (see page 49).

2. Reinstall the subsequent Orchestrators.

   See Installing an Additional Orchestrator (see page 105).

   Important: During reinstallation, the Configure button is not provided. Select the Reinstall option button instead.

3. Restart the Agents.

Chapter 6: Installing an Agent

This section contains the following topics:

Prerequisites to Installing Agents

Use the following guidelines to prepare for agent installation:

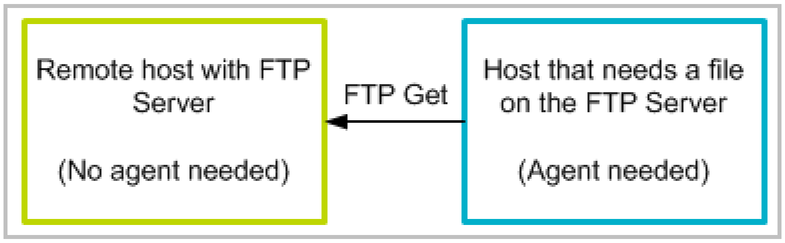
1. Identify hosts that need agents (see page 87).
2. Verify Java prerequisites for agents (see page 88).

Identify Hosts that Need Agents

In most cases, operators run on an Orchestrator. That is, the operator targets the touchpoint for an Orchestrator. Operators also run on hosts with agents. In this case, the operator targets a touchpoint associated with one or more agents.

Example: Install Agents on Hosts that Run Operators

Typically, you install CA Process Automation agents on hosts where operators execute, not on hosts that the operator connects to during execution. For example, consider a host that needs a file on the FTP server. The host that needs the file executes the FTP Get operator. An agent must be installed on the host where the operator runs. No agent is needed on the host with the FTP server


Remote host with FTP Server
(No agent needed)
FTP Get
Host that needs a file on the FTP Server
(Agent needed)

Note: When it is not possible to install an agent on a remote host where an operator must run, you can create an SSH connection from a host with an agent to the remote host. See the *Content Administrator Guide* for information on proxy touchpoints.

Verify Java Prerequisites for Agents

Before installing an agent on a host, verify that Java prerequisites are met.

Follow these steps:

1. Log on to the host. Make certain that a supported version of a Java Runtime Environment JRE is installed.   If no suitable version is present, download the JRE from the vendor and install.
2. (Optional) Set JAVA_HOME environment variable to the path of the JRE for the agent. If this variable is not set, the CA Process Automation installer prompts you to browse to the directory where JRE is installed.

Determine Port Availability for Agent

Agents and Orchestrators communicate with each other using the following ports.

- Orchestrator port: 7001
- Agent port: 7003

During agent installation, you configure the ports that agents use. When configuring network ports for an agent, accept the default settings except when:

- Another application on the host is using the default port.
- A firewall restriction prevents communication on the default port.

To use a port other than the default port, select a valid, unused port.

Install an Agent Interactively

Processes can include operators that must run on servers with a target application, database, or system. If possible, install an agent on such a server. If not possible, install the agent on a host that can connect to that server through SSH.

Important! Before you install an agent, verify that the Domain Orchestrator is running.

Follow these steps:

1. Click the Configuration tab.
2. Click the Installation palette.
3. Click Install for Install Agent.

4. 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.

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

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

6. Click Next.

   The License Agreement opens.

7. 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.

8. 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
   ```

9. Click Next.

   The Select Destination Directory page opens. On Windows hosts, the default path follows:

   ```
   C:\Program Files\CA\PAM Agent
   ```

10. 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.

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

    - (Optional) Create short cuts for all users on this host.
    - (Optional) Suppress short-cut creation entirely

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

13. 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 agent configuration.

14. 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 appears.

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

    - If you use Windows PowerShell, select the check box to set the execution policy of PowerShell to Remote Signed and browse to the PowerShell location of the host. Click Next.

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

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

    Agent installation begins.

16. Click Finish.

17. (Windows only) Start the agent service. Click Start, Programs, CA, *agent-name*, Start agent service.

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

19. Click Refresh.

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

Perform Unattended Agent Installation

CA Process Automation supports unattended agent installation to allow administrators to install agents remotely on a host computer. You can use an unattended installation to include the agent in the initial configuration routine for setting up new host computers. You can also use the unattended installation to support installation through software delivery solutions.

When you enter the domain URL with the -VdomainUrl=*domain_url*, the *domain_url* is http(s):<*FQDN_of_Domain_Orchestrator*>:<*port_number*>.

Important! The *domain_url* must be entered without **/itpam/**.

You can perform an unattended agent installation.

Follow these steps:

1. Log on as Administrator to the server where the Domain Orchestrator is installed.
2. Verify that the Domain Orchestrator is running.

   Note: An unattended agent installer must still have connectivity to the Domain Orchestrator to install an agent successfully.
3. Navigate to the following directory:

   ```
   install_dir/server/c2o/.c2orepository/media
   ```
4. Locate the file for your operating system:
   - Windows: AgentInstaller.bat
   - UNX and Linux: Agent Install.sh
   - HP-UX: AgentInstaller-hpux.sh
5. (Optional) Run the agent installer without arguments to display help.
6. Use the following command line arguments with the agent installer:

```
AgentInstaller.bat -VdomainUrl=domain_url -VacceptLicense=true [-option1 -option2
...]
AgentInstaller.sh -VdomainUrl=domain_url –VacceptLicense=true[-option1 -option2
...]
```

For example:

```
-VdomainURL=https://domainserver.company.com:8443-VcertPassword
=password
```

```
-VdomainURL=http://domainserver.company.com:8080
```

The agent installer accepts the following command line options:

–VlisteningAddress=hostname

Specifies the fully qualified domain name or IP address of the host machine on which you are installing the Agent. This is required if your host machine has multiple network interfaces.

-VdisplayName=display_name

Specifies the name that is displayed for this Agent.

-VnodePort=port_number

Specifies the port to use on the host.

-VwinService=boolean

Set the value to true to install the Agent as a Windows Service.

-Vsys.installationDir=path

Specifies the full path for installation on the host.

-VstartAgent=boolean

Set the value to true to start the Agent after the installation is complete.

-VjavaHome=<value>

Specifies the Java Home Location.

-Vscripts.tmpDir=<value>

Specifies the temporary directory to execute the scripts.

-VsetPowerShellExecPolicy=<value>

The execution of PowerShell scripts on windows platform requires execution policy setting to "Remote Signed". To run PowerShell scripts through CA Process Automation, set the value of this variable as true.

-VpowerShellPath=<value>

Specifies the PowerShell path on host machine.

Post-installation Tasks for Agents

Post-installation tasks for agents are conditional.

- If a port conflict arises after you install an agent, you can resolve port conflict for the agent (see page 93).
- If your site does not permit running agents with root privileges, you can run programs to configure agents to run as the standard low-privileged user (see page 94).

Resolve Port Conflict for an Agent

If a port becomes unavailable after an agent is installed, change the port assignment using one of the following approaches:

- **Windows**:
  1. Navigate to the following directory on the host where the agent is installed:
     ```
     agent_install_dir\.config
     ```
  2. Open the following file in an editor:
     ```
     OasisConfig.properties
     ```
  3. Modify the following port assignment:
     ```
     oasis.jxta.port=
     ```
  4. Save the file. Close the file.
  5. Navigate to the following directory on the server where the Domain Orchestrator is installed.
     ```
      install_dir/server/c2o/.system
     ```
  6. Remove the .c2o folder, if it exists.
- **UNIX or Linux**: Adjust the boot configuration.

Configure Agents to Run as the Standard Low-Privileged User

The programs described in this section apply to an agent installed on a host with a Windows operating system. These programs do the following:

- Create the standard user account used for all CA Process Automation agents.
- Assign this agent required rights on the local host.

Note: These programs have not been validated to work with all versions of Windows.

If these programs do not work on your version of Windows, configure the settings manually. Use the Group Policy Editor in the Windows Administrative Tools.

Before you begin, determine the user account *user_name* or *group_name* to use as a standard on all installed agents and Orchestrators. You can use an ordinary user account. It does not need to be a Domain account with Administrative rights.

Follow these steps:

1. Open a command prompt. For example, Run cmd.
2. Navigate to the following directory:

   ```
   agent_install_dir\PAMAgent\.c2orepository\public\tools
   ```

3. Type the following command:

   ```
   itpamsvcacct.bat user_name|group_name
   ```

   The user account is created with the name you specified.

4. Type the following five commands. (You can type a single command and use a space as a delimiter between rights.)

   ```
   itpamassgnrights.exe user_name host_name + SeTcbPrivilege
   ```

   ```
   itpamassgnrights.exe user_name host_name + SeCreateTokenPrivilege
   ```

   ```
   itpamassgnrights.exe user_name host_name + SeServiceLogonRight
   ```

   ```
   itpamassgnrights.exe user_name host_name + SeBatchLogonRight
   ```

   ```
   itpamassgnrights.exe user_name host_name +
   SeAssignPrimaryTokenPrivilege
   ```

   The user account you specified has the privileges required to run the agent on the specified local host.

How to Start or Stop an Agent

How to start and stop an agent depends on the operating system used on the host where the agent is installed.

- Microsoft Windows - Windows Service
- Unix or Linux - command line

For Windows, access the Services console from Administrative Tools in the Control Panel. From there, you can start or stop the agent service. Or, use the Start menu option. For example:

Programs > CA > CA Process Automation Agent > Start Agent Service

Programs > CA > CA Process Automation Agent > Stop Agent Service

For details on a UNIX or Linux operating system, see the following:

- Start a CA Process Automation Agent on a UNIX or Linux Host (see page 95)
- Stop a CA Process Automation Agent on a Unix or Linux Host (see page 96)

Start CA Process Automation Agent on a UNIX or Linux Host

You can start a CA Process Automation Agent on UNIX or Linux host when you see that it displays as inactive on the Agents palette.

To start a CA Process Automation Agent on a UNIX or Linux host

1. Change directories to the AGENT_HOME/pamagent.

   Note: The default location is AGENT_HOME=usr/local/CA/PAMAgent.

2. Run the following command:

   ```
   ./c2oagtd.sh start
   ```

   The agent starts running.

Stop CA Process Automation Agent on a UNIX or Linux Host

You can stop a CA Process Automation agent running on a UNIX or Linux host.

To stop CA Process Automation Agent on a UNIX or Linux host

1. Change directories to the AGENT_HOME/pamagent.

   Note: The default location is AGENT_HOME=usr/local/CA/PAMAgent

2. Run the following command:

   ```
   ./c2oagtd.sh stop
   ```

   The agent stops running.

Chapter 7: Adding a Node to the Domain Orchestrator

You can build out the CA Process Automation Domain by extending the capacity of the Domain Orchestrator. Adding a cluster node helps achieve high availability for the Domain Orchestrator.

This section contains the following topics:

Prerequisites to Installing a Cluster Node for the Domain Orchestrator

You can install a cluster node for the Domain Orchestrator. A cluster node extends the processing power of the Domain Orchestrator and therefore can improve performance. A cluster node also serves as a failover for the primary Domain Orchestrator. A cluster node shares the same databases that were configured for the primary Orchestrator.

Before installation, perform the following prerequisites:

Follow these steps:

1. Identify a host for the Orchestrator cluster node that meets platform and hardware requirements. See the Orchestrator component in the following two topics:
   - Platform Support and Requirements for CA Process Automation Components (see page 18).
   - Hardware Requirements (see page 20).
2. Verify that this host is in the same subnet as the primary Domain Orchestrator.
3. Verify that this host is in the same timezone as the primary Domain Orchestrator.
4. Verify that the host for this cluster node has a supported JDK, and if missing, download it.

   See JDK Prerequisites (see page 30).

5. If the Domain Orchestrator was configured with an F5 load balancer, add this node to the load balancer.

   See Create an F5 Node for Each Cluster Node (see page 42).

6. If the Domain Orchestrator was configured with an Apache load balancer, add this node to the load balancer.

   a. Navigate to *apache_install_location*\conf.

   b. Open the workers.properties file.

   c. Uncomment the following lines under Define Node 2 in worker.properties file.

      ```
      worker.node2.port=8009

      worker.node2.host=hostname

      worker.node2.type=ajp13

      worker.node2.lbfactor=1
      ```

   d. Change *hostname* to the host name of the server where the Domain Orchestrator node is being installed.

   e. Add “node2” to the worker.loadbalancer.balance_workers= line under Load-balancing behaviour. The entry resembles the following:

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Note: For third and subsequent nodes, follow the same instructions, but substitute the correct node number for node2, for example, node3 or node4.

   f. Restart Apache.

Install a Cluster Node for the Domain Orchestrator

Users with PAMAdmin privileges can optionally add additional cluster nodes to a Domain Orchestrator. Clustering helps to balance the processing load across the hosts that are clustered. Clustering is a good way to promote high availability. For the Domain Orchestrator to be eligible for clustering, you must have installed a Load Balancer before you installed the Domain Orchestrator.

Verify the completion of prerequisites to installing a cluster node for the Domain Orchestrator (see page 97). Then, install the cluster node.

Follow these steps:

1. Log in to the server where you plan to install this cluster node for the Domain Orchestrator
2. Browse to CA Process Automation and log in (see page 85).
3. Click the Configuration tab
4. Click the Installation palette.
5. Click Install for Install Cluster Node For Domain Orchestrator.
6. If the digital signature cannot be verified, click Run to start the installation.
7. On the Welcome to the CA Process Automation 3rd Party Installer Setup Wizard, click Next.
8. Specify the destination directory to install the Orchestrator node, and click Next.

   The installer creates the folder automatically if it does not exist.
9. On the Prerequisites for CA Process Automation Installation screen, click Next.

   The Completing the CA Process Automation Setup Wizard for prerequisites displays a Use Domain checkbox and a path. The installation process uses the information gathered from the Domain Orchestrator installation. This check box is typically not changed during installation, but if you need to enter new information, click the check box and enter the new information.
10. Click Finish to launch the installation of the cluster node for the Domain Orchestrator.
11. On the Welcome screen, click Next.
12. Accept the license agreement, and click Next.
13. Accept the displayed path or browse to the Java Home Directory. Click Next.

    The JDK is validated, and the Orchestrator installation begins. It will take a minute to copy configuration files.
14. Enter the load balancer worker node information, verify the information in the other fields prepopulated with details entered during Domain Orchestrator installation. Click Next.

Load Balancer Worker Node

Specifies the node name, for example, node 2. This is the name of this node specified in the Apache workers.properties file, where *hostname* is the name of the host on which you are installing the cluster node:

worker.**node2**.host=*hostname*.*mycompany*.com

Note: The Domain Orchestrator is node1. For the second node, type **node2.**

Public Host Name

Specifies the FQDN of the server where the load balancer is installed, that is:

loadbalancer_hostname.*mycompany*.com

15. View the Company Name, and click Next.
16. Enter the certificate password, and click Next.

    Certificate Password

    Specifies the *same* certificate password that was entered during the installation of the Domain Orchestrator.

17. Verify the entries on the General Properties for the Orchestrator. Most of the settings derived from the Domain Orchestrator installation. Click Next.

    Server Host

    Specifies the FQDN of the host where this cluster node for the Domain Orchestrator is being installed.

18. Specify a Start Menu Folder, and click Next.
19. View the PowerShell settings.
20. View the CA EEM Security settings, and click Next.
21. View the database settings for the repository (library) database, and click Next.
22. View the database settings for the runtime database, and click Next.
23. View the database settings for the reporting database, and click Next.
24. Monitor the progress messages as setup installs the cluster node for the Domain Orchestrator on the computer where you initiated the installation.
25. Click Finish.

Port Planning Prerequisites

Ports are configured during installation. When configuring network ports, accept defaults except when:

- The default port is used by another application on the host.
- A firewall restriction prevents communication on the default port.

Review the use of the following ports and plan for substitutions for any ports listed here that are in use in your network or on the applicable host. With the exception of the port for agents and for CA EEM, all other properties are stored in the OasisConfig.properties file in *install_dir*/server/c2o/.config. If a conflict occurs after installation, you can modify this file manually.

162 oasis.snmptrigger.service.port

1090 jboss.remoting.port

1098 jboss.rmi.port

1099 jboss.jndi.port

1100 jboss.ha.jndi.port

1101 jboss.ha.jndi.rmi.port

1102 jboss.mcast.jndi.autodiscovery.port

3306 oasis.database.dbport

3306 oasis.reporting.database.dbport

3306 oasis.runtime.database.port

3528 OAPort

3529 OASSLPort

3873 jboss.remoting.transport.Connector.port

4444 jboss.rmi.object.port

4445 jboss.ha.pooledinvoker.serverbind.port

4446 jboss.pooledinvoker.serverbind.port

4447 jboss.ha.rmi.object.port

4448 remoting.transport.connector.port

4457 jboss.service.binding.port

4712 jboss.tx.recovery.manager.port

4714 jboss.tx.manager.sock.pid.port

5445 jboss.jbm2.port

5446 jboss.hbm2.netty.ssl.port

5250 *default port for CA EEM*

7001 oasis.jxta.port

7003 *default port for agents*

7600 jboss.jgroups.tcp.tcp_port

7650 jboss.jgroups.tcp_sync.tcp_port

7900 jboss.messaging.datachanneltcpport

7901 jboss.messaging.controlchanneltcpport

8009 tomcat.connector.ajp.port

8080 tomcat.connector.http.port

8083 jboss.rmi.classloader.webservice.port

8093 jboss.uil.serverbind.port

8181 ucf.pax.web.http.port

8443 tomcat.secure.port

45566 jboss.mcast.ha.partition.port

45567 jboss.mcast.http.sessionreplication.port

61616 ucf.bus.port

61617 ucf.bus.http.port

Synchronize Time for a Cluster Node

A cluster node for any Orchestrator must have the exact same clock time as the primary node. Take one the following approaches to synchronize the time of all nodes in a cluster:

- Synchronize all Orchestrators and cluster nodes to a standard external time server (preferred).
- Manually synchronize the time of additional nodes to that of the primary node as follows:
  1. Verify the accuracy of the primary node time.
  2. Run the appropriate OS command on each cluster node to synchronize its time with the time of the primary node. For example, you can use command like the following for synchronizing a cluster node with the primary node.

     Windows

     ```
     net time \\primarynodename /set /yes
     ```

     Unix/Linux

     ```
     ntpdate -u primarynodename
     ```

Chapter 8: Installing an Additional Orchestrator

After installing the Domain Orchestrator, you can build out the Domain by installing additional Orchestrators. You can install multiple Orchestrators in one environment. If you create a new environment, for example, for production use, install an Orchestrator in that environment.

This section contains the following topics:

Prerequisites to Installing an Orchestrator

You can install an Orchestrator in the environment with the Domain Orchestrator or in a separate environment. Before installing an Orchestrator, perform the following prerequisites:

Follow these steps:

1. Identify a host for the Orchestrator that meets platform and hardware requirements. See the Orchestrator component in the following two topics:
   - Platform Support and Requirements for CA Process Automation Components (see page 18).
   - Hardware Requirements (see page 20).
2. Verify that the host for the Orchestrator has a supported JDK, and if missing, download it.

   See JDK Prerequisites (see page 30).

3. Identify the database server or servers to host the Runtime database and optionally, the Repository (Library) database for this Orchestrator. Consider the following factors:

   - Each Orchestrator must have its own Runtime database.
   - An Orchestrator can share the Library database of the Domain Orchestrator or have its own database.
   - Typically, all Orchestrators in the Domain use the Reporting database created for the Domain Orchestrator.
   - A database server must meet platform and hardware requirements. See the Database Server component in the following two topics:
     - Platform Support and Requirements for CA Process Automation Components (see page 18).
     - Hardware Requirements (see page 20).

4. Prepare the database server. The Runtime and Repository databases can be created on different database servers.

   See Database Server Prerequisites (see page 23).

5. Evaluate the need for a load balancer for this Orchestrator. CA Process Automation supports two methods of balancing clustered Orchestrators.

   See Apache Load Balancer Prerequisites (see page 34).

   See F5 Load Balancer Prerequisites (see page 41).

6. Identify a time server (NTP server). Configuring all Orchestrators to use the same external time server (or local time server) is the best way to ensure synchronization.

7. Ensure that the following are started before browsing to CA Process Automation to begin the installation of an Orchestrator:

   - CA EEM.
   - The load balancer, if used.
   - The Domain Orchestrator service.
   - The database server you plan to use for the Runtime database and optionally, a separate Repository (or Library) database.

Install an Orchestrator

After you install the Domain Orchestrator, you can add additional Orchestrators on other hosts. Each new environment needs at least one Orchestrator, but can have more than one Orchestrator. Multiple Orchestrators permit segmentation.

By default, the "use domain" option is checked and disabled. New Orchestrators inherit CA EEM information from the Domain Orchestrator. This check box is typically not changed during installation, but if you need to enter new information, click the check box and enter the new information.

Before installing an Orchestrator, perform prerequisites to installing an Orchestrator (see page 105). Then, install the additional Orchestrator.

Follow these steps:

1. Log on to the server where you want to install the new Orchestrator.
2. Browse to CA Process Automation and log in (see page 85). Log in with administrator credentials, for example, as a member of PAMAdmins group.
3. Click the Configuration tab and select the Installation palette.
4. Click the prerequisites link and verify that all required prerequisites have been met.
5. Click Install Orchestrator.

   If using Firefox, open with Java Web Start Launcher (default).

   If needed, install the required certificate as instructed.
6. Select a language and click OK.

   The Welcome to the CA Process Automation 3rd Party Installer Setup Wizard page appears.
7. Click Next.
8. Accept the licensing agreement, and click Next.
9. Specify the destination directory to install the Orchestrator, and click Next.

   The installer creates the folder automatically if it does not exist.
10. On the Prerequisites for CA Process Automation Installation screen, click Next.

Subsequent screens of the installer may include the Use Domain check box which is selected by default to let the installer use the information gathered from the Domain Orchestrator installation.

11. Specify JDBC jars for installation in one of the following ways:
    - Click Next to use the JCBC jars configured during Domain Orchestrator installation.
    - Clear Use Domain, click Add Files, select the database server type, click Browse and navigate to the JDBC jar file for the selected server type. Then, click Next.
12. On the confirmation screen, click Next.
13. Click Finish to move on to the CA Process Automation installer.

14. On the Welcome screen, click Next.

15. Accept the license agreement, and click Next.

16. Click Next to accept the default. If the JAVA_HOME environment variable is not set on the host, enter the directory where JDK is installed at the Java Home Directory page and click Next.

17. View the Domain URL, and click Next.

18. If you are not using a load balancer, skip this step. Otherwise, complete this page. Then click Next.

    Configure Load Balancer

    Specifies whether to install this Orchestrator with the potential for clustering.

    Selected

    Indicates that a load balancer is configured for this Orchestrator.

    Cleared

    Indicates that a load balancer is not configured for this Orchestrator.

    Load Balancer Worker Node (Apache)

    Specifies the name of this node. Since this Orchestrator is the first node in this cluster, this is **node1**.

    Public Host Name

    Specifies the public host name. For example:

    loadbalancerhost.*mycompany*.com

    - If Configure Single Sign-on (SSO) is selected, specifies the FQDN of the IIS/Apache on which the CA SiteMinder WebAgent is configured.
    - If Configure Single Sign-on(SSO) is cleared, specifies the FQDN of the load balancer.

    Public Host Port Number

    If Support Secure Communication is cleared, specifies the HTTP port for IIS/Apache, the Public Host.

    Default

    80

    Public Host Secure Port

    If Support Secure Communication is selected, specifies the HTTPS port for IIS/Apache, the Public Host.

    Default

    443

Support Secure Communication

Specifies whether the Public Host uses of HTTPS for secure communication.

Selected

Uses HTTPS.

Cleared

Does not use HTTPS; uses HTTP for basic communication.

19. View the Company Name, and click Next.
20. Enter a certificate password, and click Next.

    This is the same certificate password that was entered during the installation of the Domain Orchestrator.
21. Specify Start Menu Folder preferences and click Next.
22. Enter the General Properties for the Orchestrator, and click Next.

    Server Host

    Specifies the FQDN of this Orchestrator.

    Display Name

    Specifies the name to display for this Orchestrator in the Configuration Browser.

    - If you do not configure a load balancer, the Display Name is the same as the Server Host name.
    - If you configure a load balancer, the Display Name is the FQDN of the server where the load balancer is installed.

23. Set the temporary directory in which to execute scripts. Accept the default and click Next.
24. Set the PowerShell execution policy and click Next.
25. Enter the Repository database settings for this Orchestrator in one of the following ways:
    - Enter the same information that was configured for the Domain Orchestrator, click Test Database Settings, and then click Next.
    - Create a separate database. Complete all fields. Provide a unique name for the Repository database. Click Create Database, click Test Database Settings, and then click Next.
26. Enter the Runtime database settings. A Runtime database can be used by only one Orchestrator.
    a. If the new database uses the same database server as the Repository database for this Orchestrator, click copy from main repository to copy the defined User Name and Password.
    b. If the Database Server you specify is host to other Runtime databases, create a valid, unique name for this Runtime database.
    c. Click Create Database
    d. Click Test Database Settings
    e. Click Next.
27. View Reporting Database Settings and click Next. The Reporting database is shared by all Orchestrators in the Domain.
28. Click Finish.

Post-Installation Tasks for an Orchestrator

Perform the following post-installation tasks as needed.

1. To configure an Apache load balancer to use secure communication through SSL, take the following steps:

    a. Navigate to the following folder:
    `apache_install_dir\conf\extra\`

    b. Open the following file:
    `httpd-ssl.conf`

    c. Add the following lines inside the <VirtualHost> </VirtualHost> tags at the end of the file:

    ```
    SSLOptions +StdEnvVars +ExportCertData
    JkMount /* loadbalancer
    ```

    Note: To configure a load balancer to use basic communication, comment out the previous statement.

    d. Save the file. Close the file.

    e. Restart the Apache HTTP Server.

2. Configure ports (see page 48).

3. Configure firewalls for bi-directional communication (see page 69).

4. If you installed the Domain Orchestrator on a server with the HP-UX operating system, perform additional configuration steps on HP-UX. (see page 70)

5. (Windows only) Start the Orchestrator service.

    The Orchestrator registers itself with the Domain Orchestrator.

6. Verify the installation of the additional Orchestrator.

    a. Browse to CA Process Automation and log in.

    b. Click the Configuration tab.

    c. Click the Orchestrators node in the Configuration Browser palette.

    d. View the new Orchestrator in this list.

Chapter 9: Adding a Node to an Additional Orchestrator

After installing an additional Orchestrator, you can extend its capacity and provide failover capability by adding a cluster node. If the primary node fails, the secondary node acts as the primary node. You can use interactive installation or unattended installation when you install cluster nodes.

This section contains the following topics:

Prerequisites to Installing a Cluster Node for an Orchestrator

You can install a cluster node for an Orchestrator. A cluster node extends the processing power of an Orchestrator and therefore can improve performance. A cluster node can serve a failover function should the primary Orchestrator fail. We recommend limiting a clustered Orchestrator to two nodes: the primary Orchestrator and the cluster node. A cluster node shares the same databases that were configured for the primary Orchestrator.

Before installation, perform the following prerequisites:

Follow these steps:

1. Identify a host for the Orchestrator cluster node that meets platform and hardware requirements. See the Orchestrator component in the following two topics:
   - Platform Support and Requirements for CA Process Automation Components (see page 18).
   - Hardware Requirements (see page 20).
2. Verify that this host is in the same subnet as the primary Orchestrator.
3. Verify that this host is in the same timezone as the primary Orchestrator.
4. Verify that the host for this cluster node has a supported JDK, and if missing, download it.

   See JDK Prerequisites (see page 30).

5. If the Orchestrator was configured with an F5 load balancer, add this node to the load balancer.

   See Create an F5 Node for Each Cluster Node (see page 42).

6. If the Orchestrator was configured with an Apache load balancer, add this node to the load balancer.

   a. Navigate to *apache_install_location*\conf.

   b. Open the workers.properties file.

   c. Uncomment the following lines under Define Node 2 in worker.properties file.

   ```
   worker.node2.port=8009
   worker.node2.host=hostname
   worker.node2.type=ajp13
   worker.node2.lbfactor=1
   ```

   d. Change *hostname* to the host name of the server where the Orchestrator node is being installed.

   e. Add “node2” to the worker.loadbalancer.balance_workers= line under Load-balancing behaviour. The entry resembles the following:

   ```
   worker.loadbalancer.balance_workers=node1,node2
   ```

   Note: For third and subsequent nodes, follow the same instructions, but substitute the correct node number for node2, for example, node3 or node4.

   f. Restart Apache.

Installing a Cluster Node for an Orchestrator

Users with PAMAdmins privileges can optionally add additional cluster nodes to an Orchestrator with a load balancer.

Follow these steps:

1. Log in to the server where you plan to install this cluster node for an additional Orchestrator.
2. Browse to CA Process Automation and log in (see page 85).
3. Click the Configuration tab and click the Installation palette.
4. Click Install for *Install Cluster Node For Orchestrator*.
5. If the digital signature cannot be verified, click Run to start the installation.
6. On the Third Party Installation screen, click Next.
7. Specify the destination directory to install the Orchestrator node, and click Next.

   The installer creates the folder automatically if it does not exist.
8. On the Prerequisites for CA Process Automation Installation screen, click Next.

   A subsequent screen includes the following check box:

   Use Domain

   Specifies whether this cluster node is for the Domain Orchestrator

   Cleared - Specifies this cluster node is not for the Domain Orchestrator.

   On the confirmation screen, click Next.
9. Click Finish to move on to the CA Process Automation installer.
10. On the Welcome screen, click Next.
11. Accept the license agreement, and click Next.
12. Specify the Java Home Directory. The CA Process Automation installer will have prepopulated this field with the most recent suitable JDK it was able to locate in the path. If needed, browse to the directory where JDK is installed, and click Next.

    The JDK is validated, and the Orchestrator installation begins. This will take a minute or so as files are copied.
13. Enter the load balancer information, and click Next.

    Load Balancer Worker Node

    Specifies the name of this node as it corresponds to the name specified in the Apache workers.properties file.

    The first node in this cluster is the Orchestrator node. Name the second node as node2.

    Public Host Name

Specifies the public host name.

- If Configure Single Sign-on(SSO) is selected, this field contains the host name of the IIS/Apache on which the CA SiteMinder WebAgent is configured.

  Note: If Configure Single Sign-on(SSO) is selected, then the CA SiteMinder WebAgent must be configured with the same Apache Load Balancer.

- If an Apache load balancer is selected without the Configure Single Sign-on(SSO) option, then this field contains the hostname of the Apache Load Balancer.

Public Host Port Number

Specifies the HTTP port for IIS/Apache which is the Public Host. The default is port 80. If you change this value during the Load Balancer installation and configuration, then you will have to update this value accordingly.

Public Host Secure Port

Specifies the HTTPS port for IIS/Apache which is the Public Host. Support Secure Communication (below) must be selected.

Support Secure Communication

Select this check box if IIS/Apache, the Public Host, is configured to communicate using HTTPS.

14. View the Company Name, and click Next.
15. Enter the certificate password, and click Next.

    This is the same certificate password that was entered during the installation of the Domain Orchestrator.

16. Specify a Start Menu Folder, and click Next.
17. Enter the General Properties for the Orchestrator, and click Next.

    For more information about each property see Install and Configure the Domain Orchestrator .

18. View the Security settings, and click Next.
19. View the database settings, and click Next.
20. View the Reporting database settings, and click Next to complete the installation.
21. Click Finish.

    The cluster node for the selected Orchestrator is installed.

Synchronize Time for a Cluster Node

A cluster node for any Orchestrator must have the exact same clock time as the primary node. Take one the following approaches to synchronize the time of all nodes in a cluster:

- Synchronize all Orchestrators and cluster nodes to a standard external time server (preferred).
- Manually synchronize the time of additional nodes to that of the primary node as follows:

  1. Verify the accuracy of the primary node time.
  2. Run the appropriate OS command on each cluster node to synchronize its time with the time of the primary node. For example, you can use command like the following for synchronizing a cluster node with the primary node.

     Windows

     ```
     net time \\primarynodename /set /yes
     ```

     Unix/Linux

     ```
     ntpdate -u primarynodename
     ```

Appendix A: Using SiteMinder with CA Process Automation

CA SiteMinder provides Single Sign-On (SSO) capabilities across single- and multiple-cookie domains, letting users access applications across different Web Servers and platforms while entering their credentials only once in each session.

This section contains the following topics:

CA SiteMinder Prerequisites

Verify that your system meets the following prerequisites to install CA Process Automation with CA SiteMinder:

- A CA EEM server that is integrated with the same LDAP/AD that is used as a User Directory in the SiteMinder Policy Server.
- A CA SiteMinder Web Agent that is integrated with either IIS or Apache.

You can use the SiteMinder Apache agent only when there is an Apache-based load balancer and clustered Orchestrator. For a standalone Orchestrator, set up port forwarding from Tomcat 8080 to IIS port 80 so the SM IIS agent functions.

Note: For more information, see the CA *SiteMinder WebAgent Installation Guide*.

For security, work directly with your CA SiteMinder Administrator to understand and follow all existing guidelines for your organization's use of CA SiteMinder.

Important! You must reinstall CA Process Automation Agents (instead of merely restarting) when the Domain Orchestrator URL changes. The following changes can affect the Domain Orchestrator URL:

- Changing the Domain Orchestrator from SSO-enabled to SSO-disabled.
- Changing the Domain Orchestrator from SSO-disabled to SSO-enabled.
- Pointing the Domain Orchestrator to a different SSO server.

Configure the CA SiteMinder Policy Server Objects

To configure CA SiteMinder, access the CA SiteMinder Policy Server Administrative UI. For more information, see the *CA SiteMinder Policy Server Configuration Guide*.

Important! Before you configure CA SiteMinder for CA Process Automation, consult your CA SiteMinder Administrator. Your company may have established policies for selecting or creating Domains, naming conventions for other entities, or other site-specific security considerations.

To configure a Web Agent object to integrate with CA Process Automation:

1. Create an Agent configuration Object in the Infrastructure Section of the CA SiteMinder Administrative UI. Select either ApacheDefaultSettings or IISDefaultSettings, depending on which web agent the web servers will host.
   - Navigate to the BadUrlChars property of the Web Agent and remove "/." and "//" from the property.
   - Navigate to the IgnoreExt property and remove ".gif,.jpg,.jpeg,.png" from the property value.
   - Navigate to LogoffUri property and set it to "/itpam/Logout".
2. Create a Host Configuration Object. Select either ApacheDefaultSettings or IISDefaultSettings, depending on which web agent the web servers will host.
3. Create a user Directory Object in the Infrastructure Section of the CA SiteMinder Administrative UI.
4. Create or select a domain in the Domain section of the CA SiteMinder Administrative UI.
5. Create a Realm in the Domain section of the CA SiteMinder Policy Server UI.
6. In the new Realm, specify the correct Agent name, set the resource filter to "/itpam", and select Protected in the Default Resource Protection section.
7. In the new Realm, create a rule with Resource as "*" so that the resource looks like web_agent/itpam* and select all in the Actions section.

   Note: Specify this rule in the Policies section by adding it to an existing policy or a new policy. For more information, see the *CA SiteMinder Policy Server Configuration Guide*.
8. Create a subrealm for each of the following URLs and select Unprotected in the Default Resource Protection section:
   - /swaref.xsd
   - /genericNoSecurity
   - /images
   - /StartAgent

- /itpamclient
- /ServerConfigurationRequestServlet
- /MirroringRequestProcessor
- /soapAttachment
- /AgentConfigurationRequestServlet
- /soap
- /css
- /js

9. Create a policy in the Policies section and add the rule that you created in Step 7 to the policy.

   For more information, see the *CA SiteMinder Policy Server Configuration Guide*.

10. (Optional) Use the default values to create a custom response variable and use it as the SSO Authentication Parameter.

    a. Create a custom response attribute **pamuser** of the type WebAgent-HTTP-Header-Variable.

    b. Set the Variable Value as the parameter used for LDAP/ActiveDirectory user ID.

    c. Add this custom response to the rule mentioned in Step 9.

    Note: During the CA Process Automation installation, specify the header parameter **pamuser** as the SSO Authentication Parameter with SSO Authentication Type as **Header**. For more information, see the *CA SiteMinder Policy Server Configuration Guide*.

Integrate CA Process Automation with IIS for Single Sign-On

Note: To integrate CA SiteMinder with clustering, select the Apache SiteMinder agent.

To configure Single Sign-On with IIS

1. Have your CA SiteMinder Administrator install CA SiteMinder WebAgent on a computer that has IIS installed.
2. If IIS is configured for SSL, unzip the IIS_https_httpfolders.zip from the /SSO/IIS folder of the CA Process Automation Third-Party Prerequisites media to the home directory of the website on which CA SiteMinder is integrated.

3. Verify that the following folders are created in the home directory:
   - c2orepository +
   - itpam
   - mirroringrepository
4. Open IIS Manager and remove SSL mode from the following folders:

   In the website:
   - c2orepository
   - mirroringrepository

   In the itpam folder:
   - MirroringRequestProcessor
   - StartAgent
   - genericNoSecurity

   To remove the SSL mode:

   a. Open the properties of the corresponding folder.

   b. Select the Directory Security tab, then click Edit in the Secure communication section and clear the Require SSL Channel check box.

   Note: To integrate CA Process Automation, use the "Tomcat Redirector" filter when CA SiteMinder Web Agent is deployed on IIS.

How to Configure IIS to Redirect to Tomcat

Prerequisite

CA SiteMinder Agent should be running on the same IIS server, before configuring “Tomcat redirector” to redirect requests to CA Process Automation. For more information see the *CA SiteMinder Installation Guide*.

Follow these steps:

1. Verify that IIS web server is installed and running successfully.
2. Copy the TomcatRedirector folder to the computer on which IIS is installed, preferably in the following path:

   ```
   C:\Program Files\CA\SharedComponents
   ```

3. Edit the isapi_redirect.properties file from the bin folder to reflect the correct path if it is different.

   Example

   ```
   # Configuration file for the Jakarta ISAPI Redirector
   # The path to the ISAPI Redirector Extension, relative to the
   website
   # This must be in a virtual directory with execute privileges.
   extension_uri=/TomcatRedirector/isapi_redirect.dll
   ```

   Note: TomcatRedirector is the virtual directory name.

   ```
   # Full path to the log file for the ISAPI Redirector
   log_file=C:\Program
   Files\CA\SharedComponents\TomcatRedirector\logs\isapi_redirect.
   log
   # Log level (debug, info, warn, error or trace)
   log_level=error
   # Full path to the workers.properties file
   worker_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\workers.propert
   ies
   # Full path to the uriworkermap.properties file\
   worker_mount_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\uriworkermap.pr
   operties
   ```

4. Edit the host name in the TomcatRedirector\conf\workers.properties file to reflect the correct host name. Replace the references to localhost.

   Example:

   ```
   # statement and uncomment the three worker.ajp13w01 lines
   ###############################################################
   #######
   # The workers that jk should create and work with
   worker.list=ajp13w01
   # Defining a worker named ajp13w01 and of type ajp13
   # Note that the name and the type do not have to match.
   worker.ajp13w01.type=ajp13
   worker.ajp13w01.host=pa-w2k3
   worker.ajp13w01.port=8009
   ```

   Note: In the preceding code, pa-w2k3 is the computer on which CA Process Automation is installed.

5. Open the IIS Manager console.

6. Right-click Default web site and pick new virtual directory and reference the TomcatRedirector\bin folder you created in Step 4.

7. Navigate to the TomcatRedirector\logs folder in Windows Explorer and give all permissions to the log file in that folder to the Network Service user.

8. Right-click the virtual directory and pick properties, click “Create” beside application name, select “Scripts and Executables” for Execute permissions, and click OK.

   Note: Verify that the Application Name value is same as the Virtual directory name provided in the isapi_redirect.properties file (Step 3).

   a. Right-click Web Service Extensions, name it as TomcatRedirector, and select the path to the TomcatRedirector\bin\isapi_redirect.dll file to add a Web Service Extension. Select the Set extension status to allowed option.

   b. Recycle the IIS Admin Service

9. Add the isapi_redirect.dll as an ISAPI Filter in your IIS website. Open the IIS Manager and right-click the Web Sites folder to open the properties dialog for all web sites, select the ISAPI filter tab, click Add, and select the isapi_redirect.dll as executable.

10. Verify that requests are being forwarded to Tomcat by hitting http://localhost:80.

Integrate CA Process Automation with Apache for SSO

To configure Single Sign-On with Apache

1. Have your CA SiteMinder Administrator install CA SiteMinder WebAgent on a machine that has Apache installed on it.

2. Configure Apache with Public Host settings. For more information see Install the Domain Orchestrator (see page 53).

   Note: Contact your CA SiteMinder Administrator for more details.

Enable Logout in CA Process Automation for SSO

To enable logout in CA Process Automation for SSO

1. Navigate to the following location in the CA Process Automation installation media:

   ```
   PAM_INSTALL_DIR/server/c2o/.config
   ```

2. Double-click to open OasisConfig.propeties file and modify ALLOW_SSO_LOGOUT to true.

Appendix B: Maintain the Orchestrator DNS Name or IP Address

This section contains the following topics:

Maintain IP Addresses

The need to maintain IP addresses and or names can arise. Examples follow:

- Change IP address and name of an Orchestrator.

  Modify the name and IP address combination wherever they appear in the following files. An example install folder is C:\Program Files\CA\PAM\server\c2o.

  install_folder\.config\OasisConfig.properties

  install_folder\.config\Domain.xml

  Note: To continue to use an unchanged host name in all references in CA Process Automation, modify the DNS with the new IP address.

- If you install agents using IP address that change, reconfigure the agent by Updating the following file:

  install_folder\.config\OasisConfig.properties

  Change the value of the following property:

  ```
  oasis.jxta.host
  ```

- Use multiple IP addresses for CA Process Automation when you have two NICs, one internal, another external.

  To get CA Process Automation to bind at the external IP address, add the following property to OasisConfig.properties:

  ```
  jboss.bind.address=<x.x.x.x>
  ```

Resolve Invalid Character in CA Process Automation DNS Name

In Release 3.1, CA Process Automation accepted the installation of Orchestrators with DNS names containing restricted characters, such as underscores (_).

If you installed an Orchestrator with an invalid host name, you must take the following corrective actions:

1. Create a DNS record that maps the corrected host name to its IP address.

   See Syntax for DNS Host Names (see page 127) for standards.

2. Create a DNS record that maps the incorrect name to the corrected name.

   See Enable DNS to Resolve Invalid Host Name (see page 126).

3. Update the OasisConfig.properties file with the corrected name.

   See Maintain the DNS Host Name (see page 127).

Enable DNS to Resolve an Invalid Host Name

If you created an Orchestrator with a host name that includes an underscore or another invalid character, you can take steps that let the DNS server resolve the correct IP address from an invalid host name. This requires that you create two records in the DNS server. The first record states that the original invalid name is an alias of another canonical name.

Follow these steps:

1. In the Domain Name System, create a canonical record with new, valid host name.
2. Create a CNAME record that maps the canonical name to the original, invalid name.

Name	Type	Value
my_host.mycompany.com.	CNAME	myhost.mycompany.com.
myhost.mycompany.com	A	172.24.36.107

In this example, my_host.mycompany.com is an alias for the canonical name (CNAME) myhost.mycompany.com.

When the DNS resolver finds a CNAME record when querying for the original resource record, it restarts the query using the CNAME instead of the original name. The canonical name that a CNAME record points to can be anywhere in the DNS.

Maintain the DNS Host Name

You can modify the host name for an Orchestrator. For example, if the host name does not conform to the supported syntax, you can update it. If you installed CA Process Automation using an invalid DNS host name containing restricted characters such as underscores, create an alias that conforms to DNS standards. Then, manually replace the invalid host name with this alias in your OasisConfig.properties file.

Follow these steps:

1. Create an alias. See Enable DNS to resolve an invalid host name (see page 126).
2. Log in as an administrator to the server where the Domain Orchestrator is installed.
3. Navigate to the following folder, where install_dir refers to the path where the Domain Orchestrator is installed:

   ```
   install_dir/server/c2o/.config
   ```
4. Open the OasisConfig.properties file with an editor.
5. Use Find to locate the following property:

   ```
   oasis.local.hostname
   ```
6. Change the value for the property oasis.local.hostname=.
7. Save the file and exit.
8. Restart the Orchestrator service.
   a. Stop the Orchestrator (see page 73).
   b. Start the Orchestrator (see page 74).

Syntax for DNS Host Names

There are many places where you can enter a FQDN or an IP address. If your DNS host names include an underscore or in any way do not conform to the required syntax, specify the IP address.

Valid DNS host names:

- Begin with an alpha character.
- End with an alphanumeric character.
- Contain 2-24 alphanumeric characters.
- Can contain the special character (-) minus sign.

  Important! The minus sign (-) is the only valid special character permitted in DNS host names.

Appendix C: Troubleshooting

CA Process Automation Installation Fails

Symptom:

If an initial attempt to install CA Process Automation fails, subsequent attempts to install CA Process Automation at the same location also fail.

Solution:

To reinstall CA Process Automation, either clean up the leftover registry entries, files and folders at that location before you begin the installation, or use a different location.

Oracle DBMS May Return Corrupted Data

If you are using an Oracle DBMS there is a known Oracle defect in which concurrent inserts of CLOB data where the individual column values exceed 52K in size have caused data corruption. This has a very low frequency, and would most likely be seen under heavy load. This issue has been seen in both 10g and 11g databases.

Symptom:

CA Process Automation uses tables including columns of this type in a number of places, but the most likely scenario is the row runtime status of a process to become corrupted preventing that process from running to completion.

The related issue number from Oracle Support is 9347941

Solution:

At the time of publication this defect was still open. As a workaround, we recommend one of the following:

- See Oracle Support for a solution when you are ready to install and deploy CA Service Management, CA Process Automation, and other CA Technologies products.
- Use an alternate database server, such as MySQL or Microsoft SQL Server.

Slow Performance Using MySQL

Symptom:

When I install CA Process Automation using MySQL or Oracle as the database, I notice performance is lacking.

Solution:

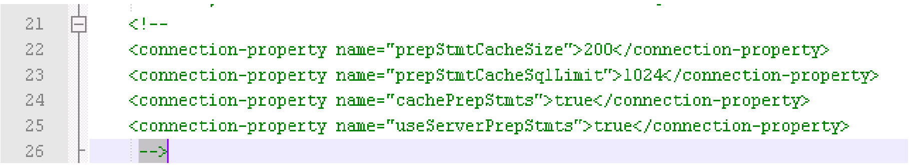
Post-installation, modify the oasis-ds.xml file to enhance CA Process Automation performance.

Do the following:

1. Locate and open the oasis-ds.xml file, located in:]

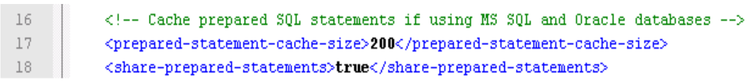
   <PAM Install Directory>\server\c2o\ext-deploy

2. Uncomment the following lines:



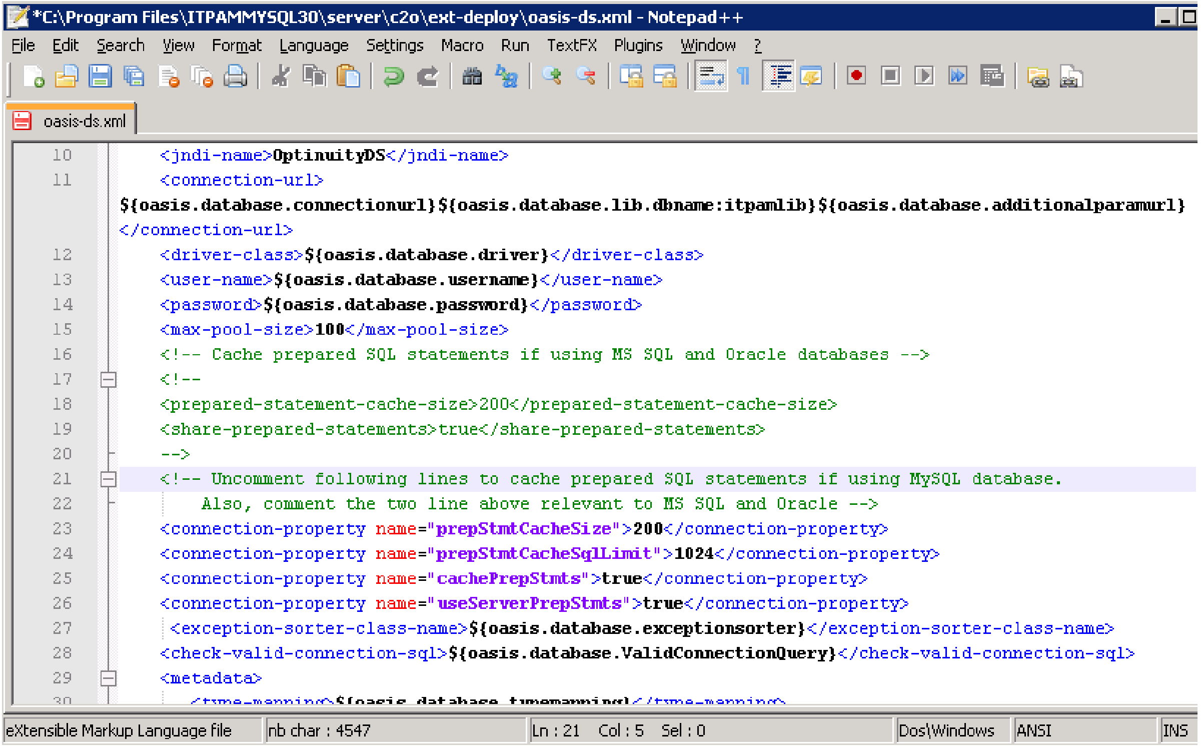
```
<!--
<connection-property name="prepStmtCacheSize">200</connection-property>
<connection-property name="prepStmtCacheSqlLimit">1024</connection-property>
<connection-property name="cachePrepStmts">true</connection-property>
<connection-property name="useServerPrepStmts">true</connection-property>
 -->
```

3. Comment the following lines:



```
<!-- Cache prepared SQL statements if using MS SQL and Oracle databases -->
<prepared-statement-cache-size>200</prepared-statement-cache-size>
<share-prepared-statements>true</share-prepared-statements>
```

The updated file should look like this:


*C:\Program Files\ITPAMMYSQL30\server\c2o\ext-deploy\oasis-ds.xml - Notepad++
File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?
oasis-ds.xml
eXtensible Markup Language file
nb char : 4547
Ln : 21 Col : 5 Sel : 0
Dos\Windows
ANSI
INS

```
    <jndi-name>OptinuityDS</jndi-name>
    <connection-url>
${oasis.database.connectionurl}${oasis.database.lib.dbname:itpamlib}${oasis.database.additionalparamurl}
</connection-url>
    <driver-class>${oasis.database.driver}</driver-class>
    <user-name>${oasis.database.username}</user-name>
    <password>${oasis.database.password}</password>
    <max-pool-size>100</max-pool-size>
    <!-- Cache prepared SQL statements if using MS SQL and Oracle databases -->
    <!--
    <prepared-statement-cache-size>200</prepared-statement-cache-size>
    <share-prepared-statements>true</share-prepared-statements>
    -->
    <!-- Uncomment following lines to cache prepared SQL statements if using MySQL database.
        Also, comment the two line above relevant to MS SQL and Oracle -->
    <connection-property name="prepStmtCacheSize">200</connection-property>
    <connection-property name="prepStmtCacheSqlLimit">1024</connection-property>
    <connection-property name="cachePrepStmts">true</connection-property>
    <connection-property name="useServerPrepStmts">true</connection-property>
     <exception-sorter-class-name>${oasis.database.exceptionsorter}</exception-sorter-class-name>
    <check-valid-connection-sql>${oasis.database.ValidConnectionQuery}</check-valid-connection-sql>
    <metadata>
        <type-mapping>${oasis.database.typemapping}</type-mapping>
```

4. Restart the Orchestrator.

Unable to Create Runtime Database

Symptom:

When I install an Orchestrator and provide the runtime database in the Runtime Database screen, the following exception is thrown:

```
The Runtime Database is being used by another orchestrator.
```

Solution:

CA Process Automation r4.0 does not allow you to share the same runtime database across Orchestrators. Typically the solution for this is to create the Runtime Database using another name, or hosted by a separate database server.

Use the following procedure **only** if you want to retain the runtime information in this database in a new CA Process Automation instance. This is rarely the case, and resetting the RuntimeDbOrchestratorID has many undesirable side effects, including making it impossible for running operators in this runtime database to complete. All agents and secondary Orchestrators must also be reinstalled, among other issues. If you have any doubt whether this procedure is appropriate for your problem, consult Technical Support before you proceed.

In this release, a new Properties table is created in the database with the following columns:

- PropKey
- PropValue

Whenever an Orchestrator uses a Runtime database, a new row is inserted in the Properties table. The PropKey is RuntimeDbOrchestratorID and the PropValue is the unique ID of the Orchestrator.

When another Orchestrator requests for the same database, the database is validated in the Properties table. If the unique ID of the requesting Orchestrator is not similar to the Propvalue, then the following message appears:

```
The Runtime Database is being used by another Orchestrator.
```

Important! The runtime database entries are not deleted even after you uninstall the product.

To use the same database again for Runtime, execute the following SQL query and delete the corresponding row form the Properties table.

```
delete from properties where propkey = 'RuntimeDbOrchestratorID'
```

Unable to Execute Run Script or Run Program Operators on RHEL6

Symptom:

The Run Script or Run Program operators fail when they are run on RHEL6.

Solution:

The Run Program and Run Script operators look for Korn shell (ksh) when they get execute on UNIX or Linux platforms. By default, RHEL 6 does not have ksh installed.

This issue can be resolved by following either of these options:

- Installing ksh:

  ksh can be installed using the following command:

  ```
  yum install ksh
  ```

- Pointing a symbolic link to a valid shell

  Create a symbolic link /bin/ksh and map the same to any shell (such as Bash) that exists on that computer. Use this command, where /bin/bash is the location of bashshell:

  ```
  ln -s /bin/bash /bin/ksh
  ```

Appendix D: Using an Embedded Mode CA Process Automation

Embedded mode is designed to install CA Process Automation with reduced prerequisites. Selecting embedded mode at installation allows you to install CA Process Automation without first installing CA EEM and an external database server. Embedded mode comes with an internal user directory and a dedicated Derby database instance as an internal database. Embedded mode CA Process Automation supports the installation of only a stand-alone Domain Orchestrator and one or more Agents (if necessary).

Important! It is not recommended to use CA Process Automation installed with embedded mode for automating processes for production use. It is preferable to install CA Process Automation with CA EEM and an external database for production use.

This section contains the following topics:

Installation Procedure

Third-party prerequisites for an embedded installation are the same as those required for a standard installation. You can install third-party prerequisites from DVD1.

The embedded mode installation process consists of the following:

1. During the Domain installation, a drop-down menu presents you with the options to select a standard installation or an embedded mode installation. Select the Embedded option.
2. An additional screen provides the parameters for Derby, such as port, host, Network Mode and the default location for Derby files.

   Note: The fields are populated with default values. CA Process Automation is functional with these values.

Important! You can convert an embedded installation of CA Process Automation to a standard CA Process Automation instance by reinstalling CA Process Automation. However, you cannot convert a standard CA Process Automation instance to an embedded mode instance.

Overview of CA Process Automation in Embedded Mode

CA Process Automation in embedded mode differs from CA Process Automation in standard mode as follows:

As an alternative to using CA EEM for user authentication and authorization, authorization information is kept in the pam-user.properties file. You can find this file in the c2o/conf/props folder. The pam-user.properties file holds the names and encrypted passwords of users.

As an alternative to external RDBMS, CA Process Automation in Embedded mode uses an internal Derby database. By default, database files are populated in the c2o/data/derby folder. The following three databases are created by default:

PAM_ LIB

The Library database stores data for automation objects created in folders in the Library tab in CA Process Automation. The stored data includes the complete definition of each object, as well as ownership, versioning information, and the library tree structure.

PAM_ RT

The Runtime database stores information about currently running process instances and historical process instances. You can access this data from the Operations tab by selecting Current or Archived. The runtime records include the state, dataset, and owner for each object instance, and scheduling information.

PAM_ REP

The Reporting database stores historical data for automation object instances, including processes, resources, schedules, and process watches. You can generate near real-time reports with this data in the Reports tab using predefined report definitions and custom report definitions.

Default Users

CA Process Automation is installed with the following default roles:

- PAMUsers, a role with login permission.
- Designers, a role with content design permissions.
- Production Users, a role with configuration permissions.
- PAMAdmins, a role with unlimited permissions.

Each default role has one default user.

Credentials for the default user for PAMUsers follow:

- Username: pamuser
- Password: pamuser

Credentials for the default user for Designers follow:

- Username: pamdesigner
- Password: pamdesigner

Credentials for the default user for Production Users follow:

- Username: pamproduser
- Password: pamproduser

Credentials for the default user for PAMAdmins follow:

- Username: pamadmin
- Password: pamadmin

Note: For more information on user permissions, see the topic Review Permissions for Default Groups in the *Content Administrator Guide*.

Encrypt and Save User Passwords

CA Process Automation uses the credentials stored in the pam-users.properties file for authenticating users when CA Process Automation is used in embedded mode. You can encrypt user passwords and then save the encrypted password with the associated user name in the pam-users.properties file.

Follow these steps:

1. Add the user ID for each CA Process Automation user in the pam-users.properties file:

   a. Navigate to the following folder:

      install_dir/c2o/conf/props

   b. Open the pam-users.properties file in an editor.

   c. Add the user ID for each user on a separate line followed by an equal sign:

      username1=

      username2=

   d. Save the file. Keep the file open.

2. Obtain a password for each user.

3. For each user password, encrypt it. Then copy and paste the encrypted value into the pam-users.properties file.

   a. Navigate to the following CA Process Automation folder:

      install_dir/c2o

   b. Locate the PasswordEncryption script:

      - Windows: PasswordEncryption.bat
      - UNIX or Linux: PasswordEncryption.sh

   c. Run the following command once for each user password:

      PasswordEncryption *passwordtoencrypt*

   d. Copy the encrypted value that this process returns.

   e. Paste the encrypted password value as the assignment for the corresponding user name. For example:

      username=encrypted_password

   f. Save the file pam-users.properties file.

4. Close the pam-users.properties file.

Index