CA Process Automation

Installation Guide

Service Pack 04.2.02

CA Technologies Product References

This document references the following CA Technologies products:

- CA Catalyst for CA Service Desk Manager (CA Catalyst Connector for CA SDM)
- CA Client Automation (formerly CA IT Client Manager)
- CA Configuration Automation (formerly CA Cohesion® Application Configuration Manager)
- CA Configuration Management Database (CA CMDB)
- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA Infrastructure Insight (formerly Bundle: CA Spectrum IM & CA NetQoS Reporter Analyzer combined)
- CA NSM
- CA Process Automation (formerly CA IT Process Automation Manager)
- CA Service Catalog
- CA Service Desk Manager (CA SDM)
- CA Service Operations Insight (CA SOI) (formerly CA Spectrum® Service Assurance)
- CA SiteMinder®
- CA Workload Automation AE

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:

- What Do You Want to Do? (see page 15)—This existing topic has a new name and has been reduced to links for various installation tasks.
- Introduction to Components of a CA Process Automation System (see page 17)—This new chapter describes each component, beginning with the ones required to set up a simple system.
  - A Simple CA Process Automation System (see page 17)
  - A Typical CA Process Automation System (see page 19)
  - A Clustered CA Process Automation System (see page 21)
  - Advanced Configuration Options (see page 22)
- The following topics were updated to reflect that the only JDK version that CA Process Automation Release 4.2 supports is JDK 1.7. This requirement applies to Orchestrators only.
  - Platform Support and Requirements for CA Process Automation Components (see page 26)
  - JDK Prerequisites (see page 93)
  - Upgrade to JDK Version 1.7
  - Upgrade to CA Process Automation Release 4.2
- Guidelines for Specifying the Database Server Name for SQL Server (see page 91)—This new topic explains that you can host a CA Process Automation database on a SQL Server named instance.
- Database Owner Privileges (see page 92)—This existing topic was corrected to include rights to act on views.
- Install the Domain Orchestrator (see page 111)—This existing topic was updated with new pages that were added to the Installation wizard for this release.
- Install an Agent Interactively (see page 186)—This existing topic was updated to document a new check box that specifies whether the agent is to use simplified communication on standard Internet ports or deprecated communication on port 7003.
- Post-installation Support for CA EEM Upgrades (see page 177)—This new topic describes how to upgrade an existing CA Process Automation Release 4.2 when you either upgrade the CA EEM release version or generate new certificates with longer key lengths.

- Example Scenario: Configure the Existing Installation to Regenerate CA Process Automation Certificates (see page 174)—This new topic provides the installation procedure to follow if the CA EEM administrator regenerates certificates with 2048 or 4096-bit keys after you install CA Process Automation with CA EEM r12.51.
- F5 Load Balancer Prerequisites (see page 52)—This existing section was modified to add changes to support simplified communication and to remove references to the Primary Node. Other changes were made to improve usability.
- NGINX Load Balancer (see page 63)—This new section documents how to configure the NGINX load balancer, which supports simplified communication. This load balancer is a good alternative to Apache, which supports only deprecated communication.
- About Agent Communication (see page 171)—This new topic describes the new simplified communication method.

- How to Upgrade CA Process Automation—This new scenario was added to the Upgrading to the Current Release chapter.
  - Take Backups and Prepare for the Outage (see page 155)—This new topic was derived from field experience with a customer upgrade.
  - Carry Out Upgrade Prerequisites (see page 156)
  - Upgrade the Domain Orchestrator (see page 158)
  - Upgrade a Nonclustered Orchestrator (see page 162)
  - Upgrade a Cluster Node (see page 164)
  - Carry out post-upgrade tasks (see page 167)—This new topic includes guidance that was derived from field experience with a customer upgrade.
  - Test Your Processes with the Upgraded Orchestrators (see page 168)
  - Switch Load Balancers from Apache to NGINX (see page 169)
  - Update F5 Pools, iRule Definition, and Configuration (see page 169)
  - Configure Agents to Use Simplified Communication (see page 170)
  - Test Your Processes with Simplified Communication (see page 136)
- Upgrade Examples—This new appendix includes:
  - Example: Upgrade a Non-clustered Orchestrator from 4.1sp01 to Release 4.2 (see page 279)—This new topic provides screenshots specific to this upgrade scenario.
  - Example: Upgrade Any Node of the Domain Orchestrator from 3.1sp01 to Release 4.2 (see page 271)—This new topic provides screenshots specific to this upgrade scenario.
  - Example: Upgrade Another Node of the Domain Orchestrator from 3.1sp01 to Release 4.2 (see page 276)—This new topic provides screenshots specific to this upgrade scenario.
- CA Process Automation Tuning (see page 225)—This new chapter provides some guidance for tuning a CA Process Automation system.
- Use CA SiteMinder with CA Process Automation (see page 229)—This existing appendix was updated to reflect integration with the CA SiteMinder Secure Policy Server (SPS).
- Ports Used by CA Process Automation (see page 235)—This new appendix lists the ports used by each components of a typical CA Process Automation system.

Contents

Chapter 5: Install the Domain Orchestrator 83

Chapter 6: Upgrade to the Current Release 153

Chapter 1: What Do You Want to Do?

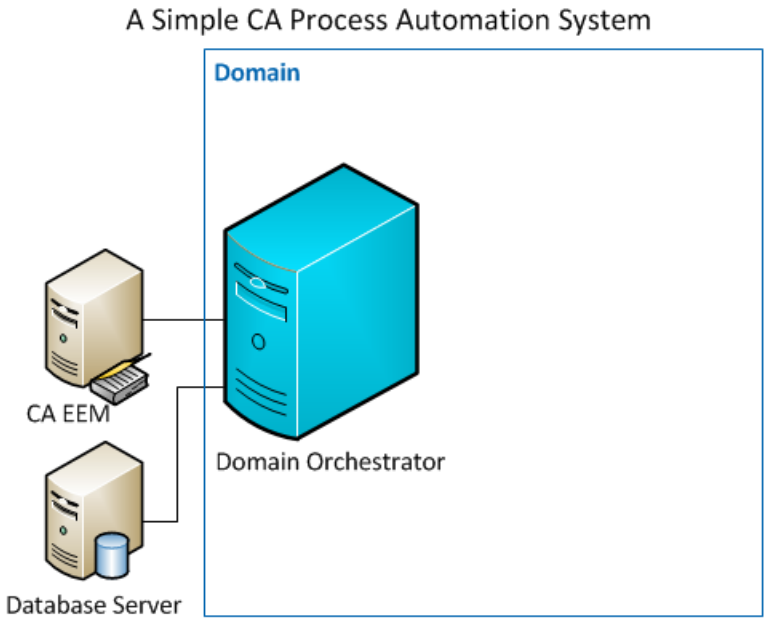
- Install CA Process Automation for the first time
  - Introduction to Components of a CA Process Automation System (see page 17).
  - Platform Support and Hardware Requirements (see page 25).
  - Install the Domain Orchestrator (see page 83).
- Upgrade CA Process Automation from a previous release (see page 153)
  - For the upgrade path to migrate an Orchestrator from a 32-bit host to a 64-bit host, see TEC596124
- Update the current CA Process Automation release to:
  - Use Multiple Active Directory Domains. (see page 177) (after upgrading CA EEM to 12.5)
  - Use new 12.5 CA EEM certificates (see page 174) (with an existing CA EEM 12.5)
  - Enable secure communications (HTTPS) (see page 181)
  - Use a new host IP address (see page 251)
  - To move or restore an Orchestrator instance, see TEC596124.
- Install an agent (see page 183).
- Build out your system
  - Set up a load balancer for Orchestrator clustering (see page 31)
  - Add a node to the Domain Orchestrator (see page 201).
  - Install an additional Orchestrator (see page 209).
  - Add a node to an additional Orchestrator (see page 219).
- Tune your system (see page 225)
- Troubleshoot (see page 255)
- Use CA SiteMinder with CA Process Automation (see page 229)

Chapter 2: Introduction to Components of a CA Process Automation System

This section contains the following topics:

A Simple CA Process Automation System

A simple CA Process Automation system includes three components: the Domain Orchestrator, a database server, and CA Embedded Entitlements Manager (CA EEM).



The Domain Orchestrator

Orchestrators are CA Process Automation servers. Users connect to an Orchestrator to design and test processes, execute processes, and configure the CA Process Automation system in various ways. Every CA Process Automation system has a Domain Orchestrator and can also have one or more non-Domain Orchestrators. A simple deployment has a single Domain Orchestrator.

A Database Server

During the installation of the Domain Orchestrator, you identify the database server in which to create the three CA Process Automation databases.

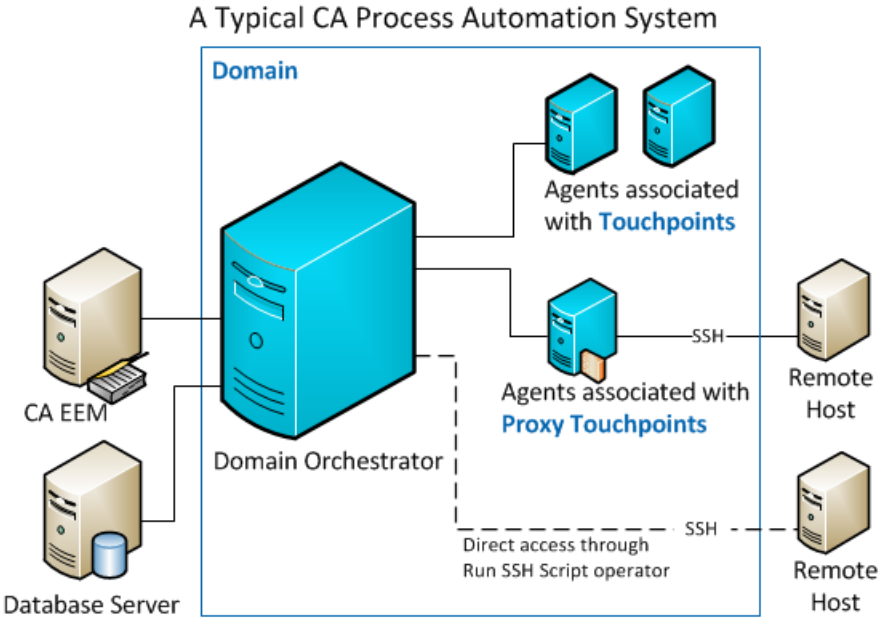
- The Library database stores the automation content that you create. Examples include processes, datasets, and forms.
- The Runtime database stores state information about process instances that have been executed or are in the process of being executed.
- The Reporting database stores information about process instances that have been executed in a format suitable for running reports against.

CA Embedded Entitlements Manager (CA EEM)

- During the installation of the Domain Orchestrator, you register the CA Process Automation application with CA EEM. A single CA EEM instance can be used with multiple CA Technologies products to provide a single place to manage user identities and their application permissions.
- CA EEM authenticates CA Process Automation users. CA EEM attempts to match credentials that users enter at login with credentials of known CA Process Automation users. All valid credentials are either defined directly in CA EEM, or, more commonly, are referenced by CA EEM from one or more LDAP-based repositories such as Microsoft Active Directory.
- CA EEM also manages the authorization levels for CA Process Automation users. Within CA EEM, you assign permissions to each user account after CA Process Automation is installed to provide that user with relevant permissions inside the CA Process Automation application.

A Typical CA Process Automation System

Many deployments require the ability to distribute some workload to be executed on hosts other than the Domain Orchestrator. Some types of workload can be executed on a remote host without an agent being installed on it. However, more functionality is available when a CA Process Automation agent is installed on the target host.



Agents

Each process instance consists of one or more operators. Each operator is targeted to run on a specific host, either directly, or indirectly using the concept of touchpoints. Each touchpoint is mapped to a specific host through system configuration.

The same touchpoint name can map to different hosts in different CA Process Automation domains or environments. Thus, touchpoints allow the same process content to be deployed unaltered in different CA Process Automation domains or environments.

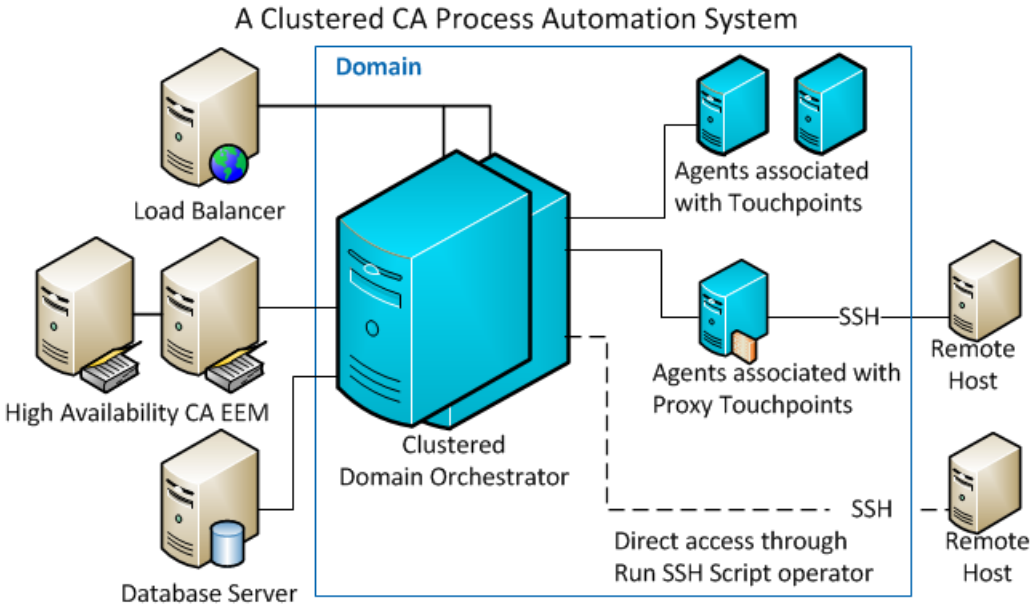
Touchpoints can map to a CA Process Automation Orchestrator or a CA Process Automation agent. Proxy touchpoints map to a remote host with no CA Process Automation software on it. Orchestrators can distribute workload to a remote host by connecting to it directly over SSH, or connecting through an agent, that in turn connects to the remote host over SSH.

Like a touchpoint, a proxy touchpoint is a logical entity. It is a name that can be used in the process designer to specify an operator execution target. While a touchpoint is defined and mapped to a specific agent through environment configuration, a proxy touchpoint is mapped to a specific agentless remote host. Each agentless remote host (mapped to a proxy touchpoint) is managed by an agent installed on a different host. When an Orchestrator distributes work that is targeting a proxy touchpoint, it sends the work to the agent that manages the remote host, and that agent in turn establishes an SSH session to the remote host to execute the work.

Consequently, the primary task of a CA Process Automation agent is to execute workload on the host on which it is installed. Additionally, agents can act as a gateway through which workload is distributed to remote hosts on which you cannot install an agent.

A Clustered CA Process Automation System

Many installations deploy a clustered Domain Orchestrator for high availability and scalability of the deployment.



Clustered Orchestrators

A clustered Orchestrator consists of two or more nodes. In normal operations, workload is shared across the nodes of the Orchestrator. Additional nodes can be added to scale out the capacity of the Orchestrator as needed. In the event of the failure of an Orchestrator node, the other nodes take over the responsibilities of the failed node until it recovers, providing High Availability.

Each Orchestrator node is installed on a different host. You install and upgrade each node separately.

Note: If you previously installed an Orchestrator initially in a standalone configuration, it is necessary to rerun the installation wizard to reconfigure it as a node of a clustered Orchestrator.

Load Balancer

CA Process Automation supports both hardware load balancers and software load balancers, for example:

- F5
- NGINX
- Apache (with functional limitations)

Note: The Apache load balancer is supported for communication between upgraded agents and a clustered Orchestrator. However, the Apache load balancer does not support the protocol that the simplified communications mechanism requires. You can continue using the deprecated communication model with Apache, but if you plan to deploy with a software load balancer, it is strongly recommended that you use NGINX.

High-availability CA EEM

CA EEM can be configured with a failover node for deployments requiring a full high availability configuration.

Advanced Configuration Options

Non-Domain Orchestrators

You can partition automation workload by deploying other Orchestrators. As with Domain Orchestrators, these non-Domain Orchestrators can be clustered.

Consider the case where certain workload must be targeted to execute in a specific datacenter or geographic region and the CA Process Automation system needs to be differently configured in each location. One approach would be to deploy an Orchestrator in each datacenter and use Orchestrator level configuration to override Domain level configuration appropriately.

Environments

A standard deployment has one Domain and a single environment, the Default Environment.

You can partition a CA Process Automation domain into multiple environments. Then, various aspects of the Domain configuration can be tailored to each environment. For example, with multiple environments you can configure things one way in a content development context and another way in a testing or production context.

Each environment can have its own Library so you can have potentially different versions of content in the different environments.

Environments also partition workload. Any given Orchestrator is associated to one environment. The Default Environment has the Domain Orchestrator and can have one or more non-Domain Orchestrators. All other environments have one or more non-Domain Orchestrators. Each Domain Orchestrator and each non-Domain Orchestrator can be clustered (multiple nodes) or nonclustered (one node).

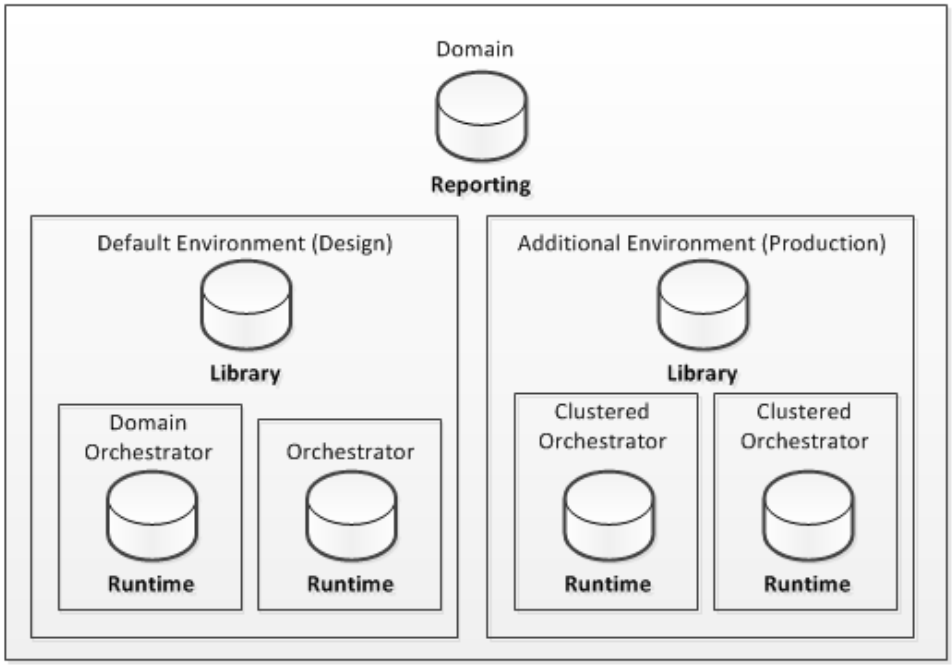
Environments can also help you partition workload within a production context. For example, a service provider could deploy one environment per customer. This setup allows running the same standard automation content across multiple environments whose workload is physically partitioned. These environments that are running the same content are configured differently and, potentially, running in different geographic locations.

Data store Implications of Adding Environments and Non-Domain Orchestrators

You have flexibility in how you assign the sharing of data stores across Orchestrators. The typical illustrated associations are:

- One Reporting data store that is shared by all Orchestrators in the Domain. While you cannot share any data store across Domains, it is possible to have more than one Reporting data store.
- A Library data store for each environment, where each Library data store is shared by all Orchestrators in the same environment.
- One Runtime data store per Orchestrator. This is a requirement. Each standalone (nonclustered) Orchestrator has its own Runtime data store. Likewise, each clustered Orchestrator uses a single Runtime data store.

Typical Database Associations



In a simple deployment with a nonclustered Domain Orchestrator in the Default Environment, the three CA Process Automation data stores are installed in one database on one database server.

Adding other environments and installing non-Domain Orchestrators significantly increases the complexity of the data store configuration required.

More information:

About CA Process Automation Data Stores (see page 87)

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.

Make sure your operating system has the latest Windows service packs or Linux updates installed.

CA Process Automation Component	Supported Operating Systems	Required Software	Other Requirements
Orchestrator	Microsoft Windows Server 2003 x64 Microsoft Windows Server 2003 R2 x64 Microsoft Windows Server 2008 x64 Microsoft Windows Server 2008 R2 x64 Microsoft Windows Server 2012 x64 Solaris SPARC 10 Solaris 11 Red Hat Enterprise Linux 5 x64, 6 x64 CentOS Linux 6 x64	Java Development Kit (JDK) 1.7 x64	See Prerequisites for Installing the Domain Orchestrator (see page 83).

CA Process Automation Component	Supported Operating Systems	Required Software	Other Requirements
Agent	Microsoft Windows Server 2003 x86/x64, 2003 R2 x86/x64, 2008 x86/x64, 2008 R2 x86/64, 2012 x86/x64 SUSE Linux Enterprise Server 10 x64, 11 x32, 11 x64 Solaris SPARC 9, 10 Solaris 10 x86, 11 Red Hat Enterprise Linux 5 x64, 6 x86, 6 x64 CentOS Linux 6 x64 AIX 6.1, 7.1 HP-UX 11i V3 (Itanium)	One of the following Java Runtime Environment (JRE) releases supported by the operating system. ■ For Windows, Solaris SPARC, and Linux: Oracle JRE 1.6 and 1.7. ■ For AIX, IBM JRE 1.6 For HP-UX, minimum HP JRE level is 1.6.0.04. **Important**! 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. Java 1.6 update 45 is the latest Java 6 version that CA Process Automation agents support.	■ For proxy touchpoints and host groups, each remote host must run an SSHv2 server. ■ Make sure that an agent installed on a UNIX or Linux machine includes ksh under the /bin/ksh directory. If ksh does not exist on the agent machine, then install it under /bin/ksh. If your agent machine already has ksh installed under a different directory, create a symbolic link (/bin/ksh) that points to the real ksh file.
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, 2012 ■ Oracle 11g R2	See Database Server Prerequisites (see page 86) for detailed requirements. For Oracle, we recommend 11.1.0.7 or 11.2.0.2 or higher.

CA Process Automation Component	Supported Operating Systems	Required Software	Other Requirements
Directory Server	See CA Embedded Entitlements Manager (CA EEM) documentation.	CA Embedded Entitlements Manager (CA EEM) r8.4 SP4 or CA EEM r12.0 -r12.51	
Browser-based UI	N/A	One of the following browsers: ■ Microsoft Internet Explorer 9x, 10 ■ Google Chrome Release 17, 18 ■ Mozilla Firefox 4.*x* through 15.0 ■ Apple Safari **Note:** If you use a Firefox or Chrome browser, disable the inline spell check feature to avoid unnecessary processing.	JavaScript enabled Adobe Flash Player

Hardware Requirements

The following table lists 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 ■ 8 GB of RAM ■ 40 GB of free disk space required ■ 100 Mbps network connection **Note:** We recommend 1000 Mbps.

CA Process Automation Component	Required Hardware
Agent	■ Host capable of running a supported OS ■ 2 GB of RAM ■ 4 GB of disk space ■ 100 Mbps network connection
Database server	See vendor specifications. Additional storage as required for the databases being hosted. **Note:** We recommend a minimum of 40 GB for your databases.
CA EEM	See the CA Embedded Entitlements 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: Set Up a Load Balancer for Orchestrator Clustering

CA Process Automation supports deprecated communication and simplified communication between agents and Orchestrators. Apache supports only deprecated communication. NGINX supports only simplified communication. F5 supports both deprecated communication and simplified communication.

If you plan to cluster an Orchestrator in the future, set up a load balancer before you install the Orchestrator, then configure the Orchestrator as node1.

This section contains the following topics:

Load Balancers and Communication

Consider the recommendations on the following table when you configure the following communication attributes:

- Install the Domain Orchestrator, Support Secure Communication: Selected is Secure; Cleared is Unsecure.
- Install an Agent Interactively, Use Deprecated Communication: Selected is Deprecated, Cleared is Simplified.

Secure or Basic (Unsecure)	Deprecated or Simplified	Recommended Load Balancers
Secure (HTTPS)	Deprecated	■ Apache (Windows) ■ Apache (UNIX/Linux) ■ F5
Secure (HTTPS)	Simplified	■ F5
Unsecure (HTTP)	Deprecated	■ Apache (Windows) ■ Apache (UNIX/Linux) ■ F5

Secure or Basic (Unsecure)	Deprecated or Simplified	Recommended Load Balancers
Unsecure (HTTP)	Simplified	■ NGINX (UNIX/Linux) ■ F5

Apache Load Balancer

The Apache load balancer does *not* support the simplified communication for agents. To take advantage of simplified communication, you must use NGINX or another web socket-based load balancer. If you use the deprecated communication method, use these instructions to install and configure the Apache load balancer.

See About Agent Communication (see page 171) for more information.

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.

Apache Load Balancer Configuration on Windows

This section provides instructions to install and configure the Apache Load Balancer on Windows.

You can configure in the following two modes:

- Basic Configuration (Windows) (see page 33)
- Secure Configuration (Windows) (see page 37)

Basic Configuration (Windows)

This section provides instructions to install and configure the Apache Load Balancer in the basic mode.

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 (Windows) (see page 33).
2. Configure basic communication (see page 35).
3. (Optional) Configure the Apache load balancer for Catalyst RESTful API (Windows) (see page 36)

   Note: For an Apache Web server to be able to forward https requests to Catalyst operators, the SSL certificates must be in PEM format. If needed, Generate SSL Certificate Files (see page 37).

Install a Load Balancer and Prepare Configuration Templates (Windows)

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

```
ApacheConfig.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 ApacheConfig.zip:

   mod-jk.conf

   httpd-proxy.conf

   uriworkermap.properties

   workers.properties

   httpd VIRTUALHOST_EXAMPLE FILE

   Note: The extracted httpd VIRTUALHOST_EXAMPLE FILE 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 following extracted files to the *apache_install_dir*\conf folder:

   mod-jk.conf

   httpd-proxy.conf

   uriworkermap.properties

   workers.properties

   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. Navigate to the following folder:

   apache_install_dir\conf

   This folder contains worker.properties and mod-jk.conf.

2. Open the workers.properties file.

3. Add the first node by defining node1 that begins with the following line:
   `worker.`**`node1`**`.host=<Enter node1 hostname here>`

4. From this line, replace the *Enter node1 hostname here* placeholder for worker.node1.host with the valid value.

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

5. Save and close the worker.properties file.

6. Open the mod-jk.conf file.

7. Uncomment the following line:

   ```
   # JkMountFile conf/uriworkermap.properties
   ```

8. Save and close the mod-jk.conf file.

9. Open the httpd.conf file.

10. Add the following entry at the end of httpd.conf file:
    ```
    #Load balancing module
    Include conf/mod-jk.conf
    ```

11. Save and close the httpd.conf file.

Configure the Apache Load Balancer for Catalyst RESTful API (Windows)

You can configure Apache Web server (load balancer) for Catalyst RESTful API. The Apache configuration changes are based on the apache load balancer that is configured for CA Process Automation already.

After you configure CA Process Automation in a cluster mode, perform the post installation tasks.

Follow these steps:

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

   install_dir\DVD1\ApacheConfTemplates

2. Extract the following files from ApacheConfig.zip:

   `httpd-proxy.conf`

3. Copy the file httpd-proxy.conf to *apacheHome*/conf/extra directory.

4. Update the following lines in both http and https Virtual Hosts to replace the Orchestrator host names for BalancerMember.

   UnSecured Node Members

   ```
   <Proxy balancer://ucfcluster>
   BalancerMember  http://< Enter node1 hostname>:7000
   BalancerMember  http://< Enter node2 hostname>:7000
   ```

   Secured Node Members

   ```
   <Proxy balancer://sslcluster>
   BalancerMember  https://< Enter node1 hostname>:7443
   BalancerMember  https://< Enter node2 hostname>:7443
   ```

5. Replace the <Enter node*x* hostname> placeholder for worker.node*x*.host with the valid value.

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

6. Save the httpd-proxy.conf file.

7. Open *apacheHome*/conf/httpd.conf file and verify that the ports 7000 and 7443 are not used.

8. Add the following line at the end of httpd.conf file:

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

9. Follow the procedure in Generate SSL Certificate Files (see page 37) to generate c2okey2.pem and c2ocert.pem files.

10. Copy the generated files to *apacheHome/*conf directory.

11. Save the modified files and restart Apache Web server.

Secure Configuration (Windows)

This section provides instructions to install and configure the Apache Load Balancer in the secure mode.

Follow these steps:

1. Install a load balancer and prepare configuration templates (see page 33).
2. Generate SSL Certificate Files (see page 37)

   Note: For an Apache Web server to be able to forward https requests to Catalyst operators, the SSL certificates must be in PEM format.
3. Configure Secure Communication (Windows) (see page 39).
4. Configure the Apache load balancer for Catalyst RESTful API (Windows) (see page 36)

Generate SSL Certificate Files

Generating the SSL certificates must be done *after* you install CA Process Automation, but *before* you configure secure communication for your load balancer. SSL certificates are not required if you want to use basic, non-secure communication for your load balancer.

Once generated, the certificate file location must be identified when you configure your load balancer configuration for secure communication.

Follow these steps:

1. Download and install OpenSSL from a third-party vendor.

   Note: Ensure that the host on which you install OpenSSL has JDK installed.

2. After you install CA Process Automation in cluster mode (and at least one node is installed), the CA Process Automation installation wizard generates the c2okeystore file in the following location:

   `\server_location\c2o\.config`

   Copy c2okeystore and paste it to the following directory:

   `\jdk_location\bin`

   You can run the commands locally from this location.

3. Use keytool in JDK to import the keystore to pksc12 format as follows:

   a. Go to the jdk_location\bin directory and run the following command:

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      The console prompts you for the destination keystore password.

      Note: The OasisConfig.properties file contains the keystore password. Locate the file in this directory:
      `\server_location\c2o\.config\`

      Open the file and copy the password. The value can be found next to the entry KEYSTOREID=.

      For example, KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. The password is 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Paste the password at the destination keystore password prompt in your open console.

   c. When prompted, re-enter the password.

   d. At the source key password prompt, enter the password again.

      A c2okeystore.p12 file is then generated in the \jdk_location\bin directory.

   e. You must convert the p12 formatted keystore to PEM formatted key and certificate files. To do this, run the openssl command at the \jdk_location\bin directory location:

      ```
      openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
      ```

   f. At the Import Password prompt, enter the keystore password.

   g. At the PEM pass phrase prompt, enter any phrase.

   h. Reenter your PEM pass phrase.

   i. Run the following command at the \jdk_location\bin directory location:
      `openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem`

j. At the Import Password prompt, enter the keystore password.

k. At the PEM pass phrase prompt, enter the phrase that you previously created for step g.

l. Reenter your PEM pass phrase.

m. Run the following command at the \jdk_location\bin directory location:
`openssl rsa -in c2okey.pem -out c2okey2.pem`

n. At the PEM pass phrase prompt, enter the phrase that you previously created for step g.

o. Reenter your PEM pass phrase.

p. Copy the c2okey2.pem and c2ocert.pem files to your load balancer's \conf directory.

Note: Make a backup of these files.

Configure Secure Communication (Windows)

You can configure a load balancer for secure communication. In the following steps, *certloc* denotes your certificate location.

Follow these steps:

1. Install a load balancer and prepare configuration templates (see page 33).
2. Open the workers.properties file.
3. Add the first node by defining node1 that begins with the following line:

   `worker.node1.host=<Enter node1 hostname here>`
4. From this line, replace the *Enter node1 hostname here* placeholder for worker.node1.host with the valid value.

   Note: The valid values are the IP address, the FQDN, or the DNS alias that resolves to the host where you are installing the initial Domain Orchestrator node. The valid value is the same value that is used for “Server Host” when installing the Domain Orchestrator.
5. Save and close the workers file.

6. Review CA default locations in the openssl file in the following directory.

   apache_install_location/conf

7. Create or get a certificate file and private key file with a “Common Name” that matches the “ServerName” in httpd.conf.

   For example, the following steps show how to use the openssl utility that is provided with the Apache load balancer to create a certificate file. Additional options control certificate expiration, file names, and algorithms. If your site has special requirements, reference the vendor-provided documentation.

   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. To do so, 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 passphrase for the PEM file and other identifying information.

      - You can accept default values for most identifying information (for example, Country Name, State or Province Name, Locality Name, Organization Name, and Organization Unit Name). To leave a field blank, enter a period (.).
      - When the Common Name prompt appears, enter the host name portion of “ServerName” as the value 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”.
      - The following fields are optional: Email address, dir, a challenge password, and an optional company name.

      The Apache load balancer creates *mypamserver.*csr and *privkey.*pem in the current directory.

   d. Create your private RSA key. To do so, enter a passphrase for *privkey*.pem when the Apache load balancer prompts you.

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

   e. Create your certificate.

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

8. Close the command prompt and open Windows Explorer to copy and delete generated files:
   a. Select the *certloc* folder or create a folder to hold your certificate and private key files.
   b. Open the *apache_install_dir*\bin folder at the location where the CERT and KEY files were generated.
   c. Drag-and-drop (that is, move) *mypamserver*.cert and *mypamserver*.key to *certloc*.
   d. Delete the intermediate files that were created in the *apache_install_dir/*bin folder. The intermediate files include *mypamserver*.CSR, *privkey*.PEM, and .RND.
9. Back up the files you created.
10. Use a text editor to 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 httpd VIRTUALHOST_EXAMPLE file that you extracted from the SecureDomainConfig_Template.zip.

```
<VirtualHost *:80>
JkMountFile conf/uriworkermap.properties
RewriteEngine on
RewriteCond %{HTTPS} on
RewriteCond https://%{HTTP_HOST}%{REQUEST_URI}
^https://.*c2orepository*|MirroringRequestProcessor*|mirror
ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
t*|ServerConfigurationRequestServlet*
RewriteRule (.*) http://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
# Load balancing module
include conf/mod-jk.conf
```

    c. Save the modified httpd.conf file and close the editor.
11. Back up the files you edited.

12. Use a text editor to modify the *apache_install_location/*conf/extra/httpd-ssl.conf configuration file as follows:
    a. Uncomment (if it is commented) the following text: “Listen 443”
    b. Change the SSLCertificateFile location to .../*certloc/mypamserver.*cert.

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

    c. Change the SSLCertificateKeyFile location to .../*certloc/mypamserver.*key.

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

    d. Add the following lines to the end of the <VirtualHost> element, before the </VirtualHost> element:

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

    e. Save the modified httpd.conf-ssl file and close the editor.
13. Restart the Apache service. To do so, click Programs, Apache HTTP Server 2.2, Control Apache Server, Restart on the Start menu.

    The changes take effect.

Apache Load Balancer Configuration on Non-Windows

This section provides instructions to install and configure the Apache Load Balancer on Non-Windows.

You can configure in the following two modes:

- Basic Configuration (Non-Windows) (see page 43)
- Secure Configuration (Non-Windows) (see page 47)

Basic Configuration (Non-Windows)

This section provides instructions to install and configure the Apache Load Balancer in the basic mode.

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 (Non-Windows) (see page 43).
2. Configure basic communication (see page 35).
3. Configure the Apache load balancer for Catalyst RESTful API (Non-Windows) (see page 45)

   Note: For an Apache Web server to be able to forward https requests to Catalyst operators, the SSL certificates must be in PEM format. If needed, Generate SSL Certificate Files (see page 37).

Install a Load Balancer and Prepare Configuration Templates (Non-Windows)

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

`ApacheConfig.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. For example, navigate to the extracted folder and run the following commands:

   ```
   ./configure -prefix=<install location>-enable-so -enable-mods-shared=all
   -enable-mod-rewrite --with-z=<zlib home>--with-included-apr  --with-mpm=worker
   --enable-ssl --with-ssl=<ssl home>
   ```

   ```
   Make
   ```

   ```
   Make install
   ```

3. Download and install the Tomcat connector to build mod_jk module. For example, navigate to *<Tomcat connector extracted location>/*native/ and run the following commands:

   ```
   ./configure --with-apxs=<install location>/bin/apxs
   make
   make install
   ```

4. Ensure the Apache server is up and running.

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

   install_dir\DVD1\ApacheConfTemplates

6. Extract the following files from ApacheConfig.zip:

   ```
   mod-jk.conf
   ```

   ```
   httpd-proxy.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

Configure the Apache Load Balancer for Catalyst RESTful API (Non-Windows)

You can configure Apache Web server (load balancer) for Catalyst RESTful API. Make the Apache configuration changes on the Apache load balancer that is configured for CA Process Automation.

Ensure that the following binaries are installed in the Apache server.

```
mod_proxy.so
mod_proxy_balancer.so
mod_proxy_http.so
```

Follow these steps:

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

   install_dir\DVD1\ApacheConfTemplates

2. Extract the following file from ApacheConfig.zip:

   `httpd-proxy.conf`

3. Copy httpd-proxy.conf to the following directory:

   `apacheHome/conf/extra`

4. Open httpd-proxy.conf and comment the following lines:

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

5. Navigate back to the *apache_install_dir*\conf folder, open httpd.conf, and uncomment the following lines (if commented):

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

6. Update the following lines in both http and https Virtual Hosts to replace the Orchestrator host names for BalancerMember.

   UnSecured Node Members

   - Node 1

     `BalancerMember  http://< Enter node1 hostname>:7000`

   - Node 2

     `BalancerMember  http://< Enter node2 hostname>:7000`

   Secured Node Members

- Node 1

  ```
  BalancerMember  https://< Enter node1 hostname>:7443
  ```

- Node 2

  ```
  BalancerMember  https://< Enter node2 hostname>:7443
  ```

7. Replace the "Enter node1 hostname here" placeholder for worker.node1.host with the valid value.

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

8. Save the httpd-proxy.conf file.
9. Open apacheHome/conf/httpd.conf file and check the port 7000 and 7443 are not used.
10. Add the following line at the end of httpd.conf file:

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

11. Generate SSL Certificate Files (see page 37) to generate c2okey2.pem and c2ocert.pem files.
12. Copy the generated files to *apacheHome*/conf directory.
13. Restart the Apache Web server.

Secure Configuration (Non-Windows)

This section provides instructions to install and configure the Apache Load Balancer in the secure mode.

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 (Non-Windows) (see page 43).
2. Configure Secure Communication (Non-Windows) (see page 47).
3. Configure the Apache load balancer for Catalyst RESTful API (Non-Windows) (see page 45)

   Note: For an Apache Web server to be able to forward https requests to Catalyst operators, the SSL certificates must be in PEM format. If needed, regenerate SSL certificate files (see page 37).

Configure Secure Communication (Non-Windows)

You can configure a load balancer for secure communication. In the following steps, *certloc* denotes your certificate location.

Follow these steps:

1. Install a load balancer and prepare configuration templates (see page 33).
2. Open the workers.properties file.
3. Add the first node by defining node1 that begins with the following line:

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

4. From this line, replace the *Enter node1 hostname here* placeholder for worker.node1.host with the valid value.

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

5. Save and close the workers file.

6. Review CA default locations in the openssl file in the following directory.

   apache_install_location/conf

7. Create or get a certificate file and private key file with a “Common Name” that matches the “ServerName” in httpd.conf.

   For example, the following steps show how to use the openssl utility that is provided with the Apache load balancer to create a certificate file. Additional options control certificate expiration, file names, and algorithms. If your site has special requirements, reference the vendor-provided documentation.

   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. To do so, type the following command where “mypamserver” is a name of your choice:

      openssl req -new -out mypamserver.csr

      You are prompted for the passphrase for the PEM file and other identifying information.

      - You can accept default values for most identifying information (for example, Country Name, State or Province Name, Locality Name, Organization Name, and Organization Unit Name). To leave a field blank, enter a period (.).
      - When the Common Name prompt appears, enter the host name portion of “ServerName” as the value 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”.
      - The following fields are optional: Email address, dir, a challenge password, and an optional company name.

      The Apache load balancer creates *mypamserver.*csr and *privkey.*pem in the current directory.

   d. Create your private RSA key. To do so, enter a passphrase for *privkey*.pem when the Apache load balancer prompts you.

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

   e. Create your certificate.

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

8. Close the command prompt and open Windows Explorer to copy and delete generated files:
   a. Select the *certloc* folder or create a folder to hold your certificate and private key files.
   b. Open the *apache_install_dir*\bin folder at the location where the CERT and KEY files were generated.
   c. Drag-and-drop (that is, move) *mypamserver*.cert and *mypamserver*.key to *certloc*.
   d. Delete the intermediate files that were created in the *apache_install_dir/*bin folder. The intermediate files include *mypamserver*.CSR, *privkey*.PEM, and .RND.
9. Back up the files you created.
10. Use a text editor to 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 httpd VIRTUALHOST_EXAMPLE file that you extracted from the SecureDomainConfig_Template.zip.

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

    c. Save the modified httpd.conf file and close the editor.
11. Back up the files you edited.

12. Use a text editor to modify the *apache_install_location/*conf/extra/httpd-ssl.conf configuration file as follows:

    a. Uncomment (if it is commented) the following text: “Listen 443”

    b. Change the SSLCertificateFile location to .../*certloc/mypamserver.*cert.

    ```
    SSLCertificateFile "/usr/local/certloc/mypamserver.cert"
    ```

    c. Change the SSLCertificateKeyFile location to .../*certloc/mypamserver.*key.

    ```
    SSLCertificateKeyFile "/usr/local/certloc/mypamserver.key"
    ```

    d. Add the following lines to the end of the <VirtualHost> element, before the </VirtualHost> element:

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

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

13. Restart the Apache service. To do so, click Programs, Apache HTTP Server 2.2, Control Apache Server, Restart on the Start menu.

    The changes take effect.

Configure Apache Load Balancer for Agent Scalability

You can configure the Apache load balancer to increase the number of agents in a cluster setup for secure and non-secure communication.

Follow these steps:

1. Make the following changes in the workers.properties file:
   - Add "uiloadbalancer" in the list of workers that are used for mapping requests as follows:

     worker.list=uiloadbalancer, loadbalancer, status
   - Add the following entries to define load balancing behaviour for UI calls:

     worker.uiloadbalancer.type=lb

     worker.uiloadbalancer.balance_workers=node1

     worker.uiloadbalancer.sticky_session=1

     worker.uiloadbalancer.retries=1
   - Change the value of the following entry to "0":

     worker.loadbalancer.sticky_session=0
2. Change the value of the following entries to "uiloadbalancer" in the uriworkermap.properties file:
   - /jmx-console
   - /jmx-console/*
   - /web-console
   - /web-console/*
   - /itpam/*
   - /itpam
   - /c2orepository/oasisHelp
   - /c2orepository/oasisHelp/*
   - /c2orepository/htmlFile/aboutUs/*
   - /c2orepository/htmlFile/language/*
   - /itpam/OasisPrimary
   - /itpam/JNLPRequestProcessor/installation
   - /itpam/clientproxy/c2oresourceaction
   - /itpam/clientproxy/c2oreportaction

Note: A new installation of CA Process Automation does not require any manual changes in the workers.properties and uriworkermap.properties files. For more information, see Install a Load Balancer and Prepare Configuration Templates (Windows) (see page 33).

F5 Load Balancer Prerequisites

Each clustered Orchestrator needs load balancing. If you have an F5 load balancer, you can use it to balance the processing of operator requests or web services requests across clustered nodes of the target Orchestrator.

Before you install the first node of a clustered Domain Orchestrator or another clustered Orchestrator, prepare F5 to perform load balancing.

First, gather the following information:

- Identity of hosts or virtual servers where Orchestrator nodes will be deployed.
- Credentials to log in to the F5 interface.

Then, configure the following F5 elements so that the elements function with CA Process Automation.

1. Create an F5 node for each cluster node (see page 53).

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

2. Create an F5 pool for each CA Process Automation cluster (see page 54).

   For CA Process Automation, each pool includes the Orchestrator cluster nodes that belong to the same clustered Orchestrator.

3. Create an F5 iRule for CA Process Automation (see page 55).

   For CA Process Automation, an iRule routes operator requests that target the touchpoint of a clustered Orchestrator.

4. Create an F5 virtual server for CA Process Automation (see page 58).

   F5 can have several virtual servers. CA Process Automation is set up as one of the virtual servers.

5. Configure F5 to use simplified communication with HTTPS (see page 60).
6. Prepare the F5 Load Balancer for Communication Verification (see page 62).
7. Enable sticky sessions on the F5 load balancer. Sticky sessions must be enabled on the F5 in order for it to work with a CA Process Automation cluster.

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 Two F5 Pools for Each CA Process Automation Cluster

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

For example, create two pools like the following examples:

- PAMPOOL set as PAMSRVRPOOL, where members use port 8080 (basic) or port 8443 (secure). This pool is used for all communications
- PAMWSPOOL set as PAMJETTYPOOL, where members use port 80 (basic) or port 443 (secure). This pool supports agents configured for simplified communication, which use web sockets.

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. Enter one of the following values for Service port based on the communication security level (Basic or Secure) and on the communication type (Deprecated or Simplified):

      Basic (Unsecure) and Deprecated communication

      8080

      Basic (Unsecure) and Simplified communication

      80 (Select HTTP, 80 is automatically populated in the Service Port field.)

      Secure and Deprecated communication

8443

Secure and Simplified communication

443 (Select HTTPS, 443 is automatically populated in the Service Port field.)

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

An iRule routes operator requests that target the touchpoint of a clustered Orchestrator. F5 creates a URL from this information and uses that URL as the touchpoint destination. To create an F5 iRule for CA Process Automation, copy the provided iRule definition into the Description text box. Then, set the values for

- PAMPOOL: Set the name for the pool that is used for both deprecated communication and simplified communication, for example "PAMSRVRPOOL"
- PAMWSPOOL: Set the name for the pool the is used for simplified (web socket) communication, for example, "PAMJETTYPOOL"
- NODE1, NODE2, and so on: Set the IP address of each node in the PAMWSPOOL
- WSPORT: The port that is used for simplified communication, either 80 (basic) or 443 (secure)

Note: An iRule identifies one Orchestrator cluster node for a request that targets the touchpoint of a clustered Orchestrator. The decision is based on the URL.

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 57) 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. Tailor the values for the set statements as needed.

- Set the PAMPOOL variable to values specific to the current pool with port as 8080 for basic (unsecure) communication.
- Set the IP addresses for NODE1 and NODE2 to values of the servers in the PAMWSPOOL pool.
- Use set WSPORT "80" for HTTP or set WSPORT "443" to use the secure (HTTPS) port for simplified communication.

```
when SERVER_CONNECTED {
IP::idle_timeout 172800000
}
when HTTP_REQUEST {
set PAMPOOL "PAMSRVRPOOL"
set PAMWSPOOL "PAMJETTYPOOL"
set NODE1 "10.130.5.146"
set NODE2 "10.130.5.147"
set WSPORT "443"
switch -glob [HTTP::uri] {
"/jmx-console*" { pool $PAMPOOL }
"/web-console*" { pool $PAMPOOL }
"/c2orepository*" { pool $PAMPOOL }
"/c2orepository/oasisHelp*" { pool $PAMPOOL }
"/c2orepository/htmlFile/aboutUs/*" { pool $PAMPOOL }
"/c2orepository/htmlFile/language/*" { pool $PAMPOOL }
"/c2orepository/htmlFile/installation/*" { pool $PAMPOOL }
"/c2orepository/media*" { pool $PAMPOOL }
"/c2orepository/thirdParty*" { pool $PAMPOOL }
"/c2orepository/MainInstallerConfiguration.properties" { pool $PAMPOOL }
"/itpam*" { pool $PAMPOOL }
"/itpam/ServerConfigurationRequestServlet" { pool $PAMPOOL }
"/itpam/MirroringRequestProcessor*" { pool $PAMPOOL }
"/itpam/AgentConfigurationRequestServlet" { pool $PAMPOOL }
"/itpam/StartAgent*" { pool $PAMPOOL }
"/itpam/OasisPrimary" { pool $PAMPOOL }
"/itpam/JNLPRequestProcessor*" { pool $PAMPOOL }
"/itpam/JNLPRequestProcessor/installation" { pool $PAMPOOL }
"/itpam/clientproxy/c2oresourceaction" { pool $PAMPOOL }
"/itpam/clientproxy/c2oreportaction" { pool $PAMPOOL }
"/mirroringrepository*" { pool $PAMPOOL }
"/birt/*" { pool $PAMPOOL }
"/ws/node1" { pool $PAMWSPOOL member $NODE1 $WSPORT }
"/ws/node1*" { pool $PAMWSPOOL member $NODE1 $WSPORT }
"/ws/node2" { pool $PAMWSPOOL member $NODE2 $WSPORT }
"/ws/node2*" { pool $PAMWSPOOL member $NODE2 $WSPORT }
"/*" { pool $PAMWSPOOL }
default { pool $PAMPOOL }
```

```
}
}
```

Important! For the 11.3.0, 11.2.1, 11.2.0, 11.1.0, 11.0.0 versions of F5 load balancer with simplified communications mode enabled for the agents, follow these steps:

1. Add the following line in the *when HTTP_REQUEST* block:

```
if { [string tolower [HTTP::header Upgrade]] contains "websocket" }{
          HTTP::disable
}
```

2. Restart the agents.

Create an F5 Virtual Server for CA Process Automation

You can create an F5 Virtual Server.

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 the associated port for the virtual server, for example, 80 for HTTP, 443 to HTTPS.

   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 clustered Orchestrator.

   Include the iRule that you created for the default pool.

   Default Pool

   Specifies the name of the pool that the virtual server routes traffic to. Specify the CA Process Automation pool as the default pool.

   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.

Configure F5 to Use Simplified Communication with HTTPS

SSL communication in F5 requires a certificate file and key file. Simplified communication can use only certificates that are generated by keytool and copied to the CA Process Automation keystore.

Follow these steps:

1. Generate SSL Certificate Files (see page 37).
2. Upload SSL certificate and key.
   a. Log in to F5.
   b. Click Local Traffic, SSL Certificates, Import.
   c. Import the key: Select Key as the Import Type, enter the Key Name, click Browse and navigate to the location of the key file, and then click Import.

      user-specified-location/c2okey2.pem

   d. Click Local Traffic, SSL Certificates, Import.
   e. Import the certificate: Select Certificate as the Import Type, enter the Certificate Name, click Browse and navigate to the location of the certificate, and then click Import.

      user-specified-location/c2ocert2.pem

3. Create the Client profile.
   a. Click Local Traffic, Profiles, SSL, Client.
   b. Click Create.
   c. Enter a name in the Name field. Accept the default for Parent Profile, clientssl.
   d. Select Advanced for Configuration.
   e. On the right hand side, select Certificate, Key, and Pass Phrase fields to make them editable.
   f. From the Certificate drop-down list, select the c2ocert2.pem certificate you imported in the previous step.
   g. From the Key drop-down list, select the c2okey2.pem key you imported in the previous step.
   h. In the Pass Phrase and in the Confirm Pass Phrase fields, enter the key phrase that was used to generate the certificate files.
   i. Click Finished.

4. Create the Server profile.
   a. Click Local Traffic, Profiles, SSL, Server.
   b. Click Create.
   c. Enter a name in the Name field. Accept the default for Parent Profile, serverssl.
   d. Select Advanced for Configuration.
   e. On the right hand side, select Certificate, Key, and Pass Phrase fields to make them editable.
   f. From the Certificate drop-down list, select the c2ocert2.pem certificate you imported in the previous step.
   g. From the Key drop-down list, select the c2okey2.pem key you imported in the previous step.
   h. In the Pass Phrase and in the Confirm Pass Phrase fields, enter the key phrase that was used to generate the certificate files.
   i. Click Finished.
5. Link the Client and Server Profiles to the F5 Virtual Server
   a. Click Local Traffic, Virtual Servers, Virtual Server List.
   b. Select the Virtual Server for CA Process Automation, for example, pamlib.

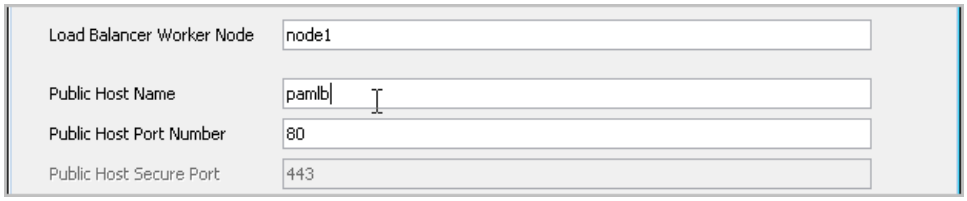
      Notice that the Service Port displays 443 and HTTPS.
   c. For SSL Profile (Client), select clientssl (the default you used for the Parent Profile in the last two steps.
   d. For SSL Profile (Server), select serverssl.
   e. Click Finished.

Comparison of port settings for HTTPS and HTTP

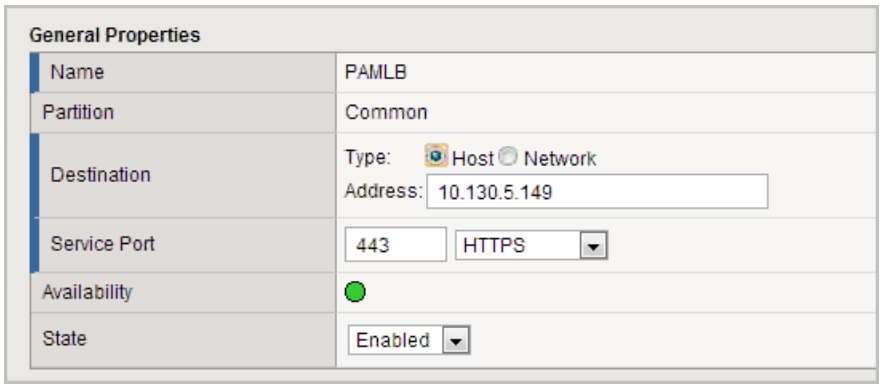
	HTTPS (secure)	HTTP (basic)
Service Port	443	80
Node members added to the pool	8443	8080
iRule referring to the web socket port	443	80

Prepare the F5 Load Balancer for Communication Verification (Example)

The Orchestrator installation process presents a configuration page where you can elect to configure a load balancer:



For Public Host Name in the CA Process Automation installation, you enter the host name that you define in F5. To validate that CA Process Automation can communicate with the host specified for Public Host Name, the CA Process Automation installation process submits an HTTP Get request to the target you specify. The problem for the CA Process Automation installation process is that this host name is mapped to the private IP address of the virtual server that F5 allocates--an IP address that is not part of your local CA Process Automation network. In the following example, 10.130.5.149 is an IP address that is part of the F5 network, not the CA Process Automation network.



Without a workaround, an error similar to the following occurs:

```
java.net.UnknownHostException:pamlb
```

To enable the communication validation to complete successfully, create an entry in your hosts file that maps your entry for Public Host Name to an IP address of a server that can respond to this request.

For example, create a hosts file entry that maps your Public Host Name entry to the IP address of a server in the CA Process Automation network with an Apache load balancer installed.

```
xxx.xxx.xxx.xxx     pamlb
```

After the installer proceeds past the load balancer page, remove this workaround line from the hosts file.

Note: Alternatively, you can configure the F5 so that the allocated IP address can accept the 'open http stream' request from the CA Process Automation Orchestrator installation process. See the F5 documentation for details.

More information:

Ports Used by the Load Balancer (see page 238)

NGINX Load Balancer

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 NGINX HTTP Server, is required for clustering any Orchestrator, including the Domain Orchestrator. A load balancer is not part of the CA Process Automation installation. You must install and configure a load balancer before you install CA Process Automation.

The simplified communication mode, introduced in CA Process Automation 4.2, uses web sockets and HTTP to produce a one way, persisted connection from the agent to the Orchestrator. CA Technologies supports NGINX for this new simplified communication method, but you can use any load balancer that supports web sockets to use it.

Note: The Apache load balancer does *not* support the simplified communication mode for agents, so use NGINX or another web socket-based load balancer to take advantage of this feature. If you are not using the simplified communication method and want to use the deprecated communication method, you can install the Apache load balancer.

Install the NGINX load balancer on a host external to CA Process Automation to ensure operating system compatibility. See the NGINX documentation for supported operating systems.

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

Important! If you want to cluster an existing stand-alone Orchestrator, install and configure a load balancer, and then reinstall the Orchestrator.

Prerequisites

Prerequisites for using the NGINX load balancer are as follows.

Install NGINX

NGINX is free open source web server software that you can download and install for your operating system. CA Process Automation is certified with NGINX version 1.4.1. Use the following instructions to get started.

Windows

Download the NGINX package and extract the files.

Linux

Note: UNIX and Linux commands for NGINX can vary, depending on your version. See the OS and NGINX documentation if you need more information or for troubleshooting.

Download the NGINX package and extract the files.

For both Windows and Linux, invoke NGINX using a command prompt.

In Windows, navigate to the NGINX directory location and enter:

```
nginx.exe
```

In Linux, enter:

```
service nginx  start
```

To verify that NGINX was successfully installed and currently running, access the URL from a browser:

```
http://hostname:80
```

Copy the Configuration Templates

Once NGINX is installed, extract the template files from the CA Process Automation installation media to your NGINX installation directory.

Follow these steps:

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

   install_dir/DVD1/NginxConfTemplates
2. Extract the files from NginxConfig.zip.
3. Navigate to the pam subfolder. This folder includes the following files:

   pam-server.conf

   Used for non-secure configuration (HTTP).

   secure-pam-server.conf

   Used for secure configuration (HTTPS).

   pam-rest.conf

   Used for REST configuration (enables the inbound PAM Rest interface).

   These files are specific to CA Process Automation configuration with NGINX.
4. Copy the required file and paste them into the following folder:

   nginx_install_dir/conf

   You can now configure the NGINX load balancer.

Basic Communication

The following instructions describe how to configure basic, non-secure communication for NGINX on Windows and Linux systems.

Windows

Follow these steps:

1. Navigate to the following folder.

   nginx_install_dir/conf

   This folder contains pam-server.conf file.

2. Open the pam-server.conf file.

3. There are four code blocks that require editing for every node that you add.

   a. Add the node1 host name in the **upstream loadbalancer** block:
   `server <Enter node1 hostname here>:<http port> max_fails=3 fail_timeout=3s`

   Note: Defines the HTTP port that is used for the web server if the Support Secure Communication check box is cleared. This port is part of the URL that is used to access CA Process Automation web services and the CA Process Automation login screen.

   b. Add the node1 host name under the **upstream jettyloadbalancer** block.
   `server <Enter node1 hostname here>:<server port> max_fails=3 fail_timeout=3s`

   c. Add the node1 host name under the **Define node1** block:
   `server <Enter node1 hostname here>:<server port> max_fails=1 fail_timeout=3s`

   Note: Defines the port that the Domain Orchestrator uses to communicate with other Orchestrators and agents.

   d. Add the node1 host name under the **upstream uiloadbalancer** block:
   `server <Enter node1 hostname here>:<http port> max_fails=3 fail_timeout=3s`

   Replace the *Enter node1 hostname here* placeholders with a valid value. Do not change the port numbers unless you use a different port for the CA Process Automation node. By default, the http port is configured to 8080 and the server port is configured to 80.

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

   Repeat these steps for each additional node that you install.

4. Save and close the pam-server.conf file.

5. Open the *nginx_install_dir*/conf/nginx.conf file.

6. Add the following entry in the http block at the end of nginx.conf file:

   `include` **`nginx_install_dir/conf/pam-server.conf;`**

This entry links NGINX with the configuration changes you made for CA Process Automation in the pam-server.conf file.

7. Save and close the nginx.conf file.

   Important! Perform the rest of these steps *after* you install at least one Orchestrator node. See Interactive Domain Orchestrator Installation (see page 108) or Unattended Domain Orchestrator Installation (see page 131) for instructions.

8. Stop NGINX. In a command prompt, navigate to the NGINX directory location and enter:

   ```
   nginx –s stop
   ```

9. Restart NGINX.

   The changes take effect.

Linux

Follow these steps:

1. Navigate to the following folder

   nginx_install_dir/conf

   This folder contains nginx.conf file.

2. Open the nginx.conf file.

3. Provide the server block as follows to verify the standalone NGINX.

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Save the file and close it.

5. Navigate to the following folder

   nginx_install_dir/conf

   This folder contains pam-server.conf file.

6. Open the pam-server.conf file.

7. There are four code blocks that require editing for every node that you add.

   a. Add the node1 host name in the **upstream loadbalancer** block:
   `server <Enter node1 hostname here>:<http port> max_fails=3 fail_timeout=3s`

   Note: Defines the HTTP port that is used for the web server if the Support Secure Communication check box is cleared. This port is part of the URL that is used to access CA Process Automation web services and the CA Process Automation login screen.

   b. Add the node1 host name under the **upstream jettyloadbalancer** block.
   `server <Enter node1 hostname here>:<server port> max_fails=3 fail_timeout=3s`

   c. Add the node1 host name under the **Define node1** block:
   `server <Enter node1 hostname here>:<server port> max_fails=1 fail_timeout=3s`

   Note: Defines the port that the Domain Orchestrator uses to communicate with other Orchestrators and agents.

   d. Add the node1 host name under the **upstream uiloadbalancer** block:
   `server <Enter node1 hostname here>:<http port> max_fails=3 fail_timeout=3s`

Replace the *Enter node1 hostname here* placeholders with a valid value. Do not change the port numbers unless you use a different port for the CA Process Automation node. By default, the server port is configured to 8080 and the jetty server port is configured to 80.

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

Repeat these steps for each additional node that you install.

8. Save and close the pam-server.conf file.
9. Open the nginx.conf file.
10. Add the following entry in the http block at the end of nginx.conf file:

    `include nginx_install_dir/conf/pam-server.conf;`

    This entry links NGINX with the configuration changes you made for CA Process Automation in the pam-server.conf file.
11. Remove the following entry:

    `include nginx_install_dir/nginx/conf.d/*.conf;`
12. Save and close the nginx.conf file.

    Important! Perform the rest of these steps *after* you install at least one Orchestrator node. See Interactive Domain Orchestrator Installation (see page 108) or Unattended Domain Orchestrator Installation (see page 131) for instructions.
13. Once you have installed at least one Orchestrator node, open the *nginx_install_dir*/conf/nginx.conf file.
14. Restart NGINX. In a command prompt, enter:

    `service nginx  restart`

    The changes take effect.

Secure Communication

The following instructions describe how to configure secure communication for NGINX on Windows and Linux systems. Secure communication differs from basic in that it requires the use of certificates and key files.

Windows

Secure communication for NGINX requires SSL certificates (c2okey2.pem and c2ocert.pem files). Make sure you generate these files (see page 37) before you begin this procedure.

Follow these steps:

1. Navigate to the following folder:

   nginx_install_dir/conf

   This folder contains secure-pam-server.conf file.

2. Open the secure-pam-server.conf file.

3. There are five code blocks that require editing for every node that you add. Edit the blocks according to your security measures.

   Note: When you select Support Secure Communication check box, this field specifies the port used in the URL that accesses CA Process Automation Web services and the browser-based CA Process Automation UI.

   a. Add the node1 host name under the **upstream uiloadbalancer** block:
   ```
   server <Enter node1 hostname here>:<https port> max_fails=3
   fail_timeout=3s
   ```

   b. Add the node1 host name in the **upstream loadbalancer** block:
   ```
   server <Enter node1 hostname here>:<https port> max_fails=3
   fail_timeout=3s
   ```

   c. Add the node1 host name under the **upstream repositoryloadbalancer** block:
   ```
   server <Enter node1 hostname here>:<https port> max_fails=3
   fail_timeout=3s
   ```

   d. Add the node1 host name under the **upstream jettyloadbalancer** block.
   ```
   server <Enter node1 hostname here>:<server port> max_fails=3
   fail_timeout=3s
   ```

   e. Add the node1 host name under the **Define node1** block:
   ```
   server <Enter node1 hostname here>:<server port> max_fails=1
   fail_timeout=3s
   ```

   Note: Defines the port that the Domain Orchestrator uses to communicate with other Orchestrators and agents.

   Replace the *Enter node1 hostname here* placeholders with a valid value. Do not change the port numbers unless you use a different port for the CA Process Automation node. By default, the https port is configured to 8443 and the server port is configured to 443.

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

Repeat these steps for each additional node that you install.

4. Update the following lines by specifying the location of c2ocert.pem and c2okey2.pem files (in the nginx_installed_location\conf directory).

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   For example:

   ```
   ssl_certificate      <nginx_install_dir\conf\c2ocert.pem>;
   ```

5. Save and close the secure-pam-server.conf file.
6. Open the nginx.conf file.
7. Add the following entry in the http block at the end of the nginx.conf file:
   `include` *`nginx_install_dir`*`/conf/secure-pam-server.conf;`

   This entry links NGINX with the configuration changes you made for CA Process Automation in the secure-pam-server.conf file.
8. Save and close the nginx.conf file.

   Important! Perform the rest of these steps *after* you install at least one Orchestrator node. See Interactive Domain Orchestrator Installation (see page 108) or Unattended Domain Orchestrator Installation (see page 131) for instructions.
9. Stop NGINX. In a command prompt, navigate to the NGINX directory location and enter:

   ```
   nginx –s stop
   ```

10. Restart NGINX.

    The changes take effect.

Linux

Secure communication for NGINX requires SSL certificates (c2okey2.pem and c2ocert.pem files). Make sure you generate these files (see page 37) before you begin this procedure.

Follow these steps:

1. Navigate to the following folder

   nginx_install_dir/conf

   This folder contains nginx.conf file.

2. Open the nginx.conf file.

3. Provide the server block as follows to verify the standalone NGINX.

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Save the file and close it.

5. Navigate to the following folder:

   nginx_install_dir/conf

   This folder contains secure-pam-server.conf file.

6. Open the secure-pam-server.conf file.

7. There are five code blocks that require editing for every node that you add. Edit the blocks according to your security measures.

   Note: When you select Support Secure Communication check box, this field specifies the port used in the URL that accesses CA Process Automation Web services and the browser-based CA Process Automation UI.

   a. Add the node1 host name under the **upstream uiloadbalancer** block:
   `server <Enter node1 hostname here>:<https port> max_fails=3 fail_timeout=3s`

   b. Add the node1 host name in the **upstream loadbalancer** block:
   `server <Enter node1 hostname here>:<https port> max_fails=3 fail_timeout=3s`

   c. Add the node1 host name under the **upstream repositoryloadbalancer** block:
   `server <Enter node1 hostname here>:<https port> max_fails=3 fail_timeout=3s`

   d. Add the node1 host name under the **upstream jettyloadbalancer** block.
   `server <Enter node1 hostname here>:<server port> max_fails=3 fail_timeout=3s`

   e. Add the node1 host name under the **Define node1** block:
   `server <Enter node1 hostname here>:<server port> max_fails=1 fail_timeout=3s`

   Note: Defines the port that the Domain Orchestrator uses to communicate with other Orchestrators and agents.

   Replace the *Enter node1 hostname here* placeholders with a valid value. Do not change the port numbers unless you use a different port for the CA Process Automation node. By default, the server port is configured to 8443 and the jetty server port is configured to 443.

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

   Repeat these steps for each additional node that you install.

8. Update the following lines by specifying the location of c2ocert.pem and c2okey2.pem files (in the nginx_installed_location\conf directory).

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   For example:

   ```
   ssl_certificate      <nginx_install_dir\conf\c2ocert.pem>;
   ```

9. Save and close the secure-pam-server.conf file.
10. Open the nginx.conf file.
11. Add the following entry in the http block at the end of nginx.conf file:

    `include nginx_install_dir/conf/secure-pam-server.conf;`

    This entry links NGINX with the configuration changes you made for CA Process Automation in the secure-pam-server.conf file.
12. Remove the following entry from:

    `include nginx_install_dir/nginx/conf.d/*.conf;`
13. Save and close the nginx.conf file.

    Important! Perform the rest of these steps *after* you install at least one Orchestrator node. See Interactive Domain Orchestrator Installation (see page 108) or Unattended Domain Orchestrator Installation (see page 131) for instructions.
14. Once you have installed at least one Orchestrator node, open the *nginx_install_dir*/conf/nginx.conf file.
15. Restart NGINX. In a command prompt, enter:

    `service nginx  restart`

    The changes take effect.

REST Configuration

CA Process Automation provides the option to configure an NGINX load balancer for Catalyst RESTful API. The following instructions describe how to configure your NGINX load balancer to use REST for basic and secure communication on both Windows and Linux systems.

Basic Communication

Follow these steps:

1. Navigate to the following folder

   nginx_install_dir/conf

   This folder contains pam-rest.conf file.

2. Open the pam-rest.conf file.

3. Edit the following block of code:

   ```
   HTTP
   upstream ucfcluster  {
     server <Enter node1 hostname here>:7000 max_fails=3
   fail_timeout=5s;
     server <Enter node2 hostname here>:7000 max_fails=3
   fail_timeout=5s;
   }
   ```

   Replace the *Enter node1 hostname here* placeholders with a valid value. Do not change the port numbers unless you use a different port for the CA Process Automation node.

   Repeat these steps for each additional node that you install.

4. Save and close the pam-rest.conf file.

5. Open the nginx.conf file.

6. Add the following entry in the http block at the end of the nginx.conf file:
   `include` *nginx_install_dir*`/conf/pam-rest.conf;`

   This entry links NGINX with the configuration changes you made for CA Process Automation in the pam-rest.conf file.

7. Save and close the nginx.conf file.

   Important! Perform the rest of these steps *after* you install at least one Orchestrator node. See Interactive Domain Orchestrator Installation (see page 108) or Unattended Domain Orchestrator Installation (see page 131) for instructions.

8. Once you have installed at least one Orchestrator node, open the *nginx_install_dir*/conf/nginx.conf file.

9. Save and close the nginx.conf file.

10. Stop NGINX. In a command prompt, navigate to the NGINX directory location and enter:

    - Windows:
      `nginx –s stop`
    - Linux:
      `service nginx  stop`

11. Restart NGINX.

The changes take effect.

Secure Communication

SSL certificate files are required for secure communication with REST. Make sure you generate these files (see page 37) before you begin this procedure.

Follow these steps:

1. Navigate to the following folder

   nginx_install_dir/conf

   This folder contains pam-rest.conf file.

2. Open the pam-rest.conf file.

3. Edit the following block of code:

   ```
   ## HTTPS
   upstream sslcluster  {
     server <Enter node1 hostname here>:7443 max_fails=3
   fail_timeout=5s;
     server <Enter node2 hostname here>:7443 max_fails=3
   fail_timeout=5s;
   }
   ```

   Replace the *Enter node1 hostname here* placeholders with a valid value. Do not change the port numbers unless you use a different port for the CA Process Automation node.

   Repeat these steps for each additional node that you install.

4. Update the following lines by specifying the location of c2ocert.pem and c2okey2.pem files (in the nginx_installed_location\conf directory).

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   For example:

   ```
   ssl_certificate      <nginx_install_dir\conf\c2ocert.pem>;
   ```

5. Save and close the pam-rest.conf file.

6. Open the nginx.conf file.

7. Add the following entry in the http block at the end of the nginx.conf file:
   `include nginx_install_dir/conf/pam-rest.conf;`

   This entry links NGINX with the configuration changes you made for CA Process Automation in the pam-rest.conf file.

8. Save and close the nginx.conf file.

   Important! Perform the rest of these steps *after* you install at least one Orchestrator node. See Interactive Domain Orchestrator Installation (see page 108) or Unattended Domain Orchestrator Installation (see page 131) for instructions.

9. Once you have installed at least one Orchestrator node, open the *nginx_install_dir*/conf/nginx.conf file.

10. Save and close the nginx.conf file.

11. Stop NGINX. In a command prompt, navigate to the NGINX directory location and enter:

    - Windows:
      `nginx –s stop`
    - Linux:
      `service nginx  stop`

12. Restart NGINX.

    The changes take effect.

Configure NGINX Load Balancer for Agent Scalability

You can configure NGINX load balancer to increase the number of agents in a cluster setup for secure and non-secure communication.

Follow these steps:

1. Navigate to the folder (for example, nginx_install_dir/conf/NGINX.conf) that contains the NGINX.conf file.
2. Add the worker_rlimit_nofile property and set the value to 30000 in the NGINX.conf file.
3. Add the accept_mutex property in the NGINX.conf file as follows:

   ```
   events {
       accept_mutex off;}
   ```
4. Edit the worker_connections and the worker_processes property value in the NGINX.conf file based on the following factors:

   - Number of agents you want to install
   - Number of processors

   wherein:

   - worker_connections: Indicates the maximum number of simultaneous connections that a worker process establishes.
   - worker_processes: Indicates the optimal value that depends on the number of CPU cores.

   For example:

   To find out the number of cores in your setup; enter the following command using the Linux Shell prompt:

   grep processor /proc/cpuinfo | wc –l

   Assuming the value that is returned from the command is "2". That means, the number of CPU cores in the server of your setup is 2.

   The value of worker_connections is calculated as follows:

   Wc = 2NA/Wp

   Where:

   N=Total number of nodes in a cluster.

   A=Total number of agents you want to install.

   Wp=Total number of CPU processors as calculated in step 4.

   - Example 1:

     When you want to install 4000 agents in a two-node cluster setup and the number of CPU cores in the server of your setup is 2, edit the worker_processes property to 2.

Substituting the values in the formula:

Wc = 2*2*4000)/2

To install 4000 agents, edit the worker_connections property to 8000.

- Example 2:

  When you want to install 2500 agents with a standalone orchestrator and the number of CPU cores in the server of your setup is 4, edit the worker_processes property to 4.

  Substituting the values in the formula:

  Wc = 2*1*2500/4

  To install 2500 agents, edit the worker_connections property to 1250.

- Example 3:

  When you want to install 3000 agents in a three-node cluster setup and the number of CPU cores in the server of your setup is 1, edit the worker_processes property to 1.

  Substituting the values in the formula:

  Wc = 2*3*3000/1

  To install 3000 agents, edit the worker_connections property to 18000.

5. Restart the NGINX load balancer.

Generate SSL Certificate Files

Generating the SSL certificates must be done *after* you install CA Process Automation, but *before* you configure secure communication for your load balancer. SSL certificates are not required if you want to use basic, non-secure communication for your load balancer.

Once generated, the certificate file location must be identified when you configure your load balancer configuration for secure communication.

Follow these steps:

1. Download and install OpenSSL from a third-party vendor.

   Note: Ensure that the host on which you install OpenSSL has JDK installed.

2. After you install CA Process Automation in cluster mode (and at least one node is installed), the CA Process Automation installation wizard generates the c2okeystore file in the following location:

   `\server_location\c2o\.config`

   Copy c2okeystore and paste it to the following directory:

   `\jdk_location\bin`

   You can run the commands locally from this location.

3. Use keytool in JDK to import the keystore to pksc12 format as follows:

   a. Go to the jdk_location\bin directory and run the following command:

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      The console prompts you for the destination keystore password.

      Note: The OasisConfig.properties file contains the keystore password. Locate the file in this directory:
      `\server_location\c2o\.config\`

      Open the file and copy the password. The value can be found next to the entry KEYSTOREID=.

      For example, KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. The password is 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Paste the password at the destination keystore password prompt in your open console.

   c. When prompted, re-enter the password.

   d. At the source key password prompt, enter the password again.

      A c2okeystore.p12 file is then generated in the \jdk_location\bin directory.

   e. You must convert the p12 formatted keystore to PEM formatted key and certificate files. To do this, run the openssl command at the \jdk_location\bin directory location:

      ```
      openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
      ```

   f. At the Import Password prompt, enter the keystore password.

   g. At the PEM pass phrase prompt, enter any phrase.

   h. Reenter your PEM pass phrase.

   i. Run the following command at the \jdk_location\bin directory location:
      `openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem`

j. At the Import Password prompt, enter the keystore password.

k. At the PEM pass phrase prompt, enter the phrase that you previously created for step g.

l. Reenter your PEM pass phrase.

m. Run the following command at the \jdk_location\bin directory location:
`openssl rsa -in c2okey.pem -out c2okey2.pem`

n. At the PEM pass phrase prompt, enter the phrase that you previously created for step g.

o. Reenter your PEM pass phrase.

p. Copy the c2okey2.pem and c2ocert.pem files to your load balancer's \conf directory.

Note: Make a backup of these files.

Chapter 5: Install 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 in either of the following ways:

- Interactive installation with a wizard (physical display is required).
- Unattended installation: 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

Consider configuring a load balancer for your first installation to prepare for later expansion. (Adding cluster nodes can be done when the need arises.)

Note: We recommend a hardware load balancer. See F5 Load Balancer Prerequisites (see page 52). If this is not possible, we recommend NGINX as the software load balancer of choice. NGINX for UNIX is highly scalable. See NGINX Load Balancer Prerequisites.

Plan your initial CA Process Automation installation. For component requirements, see:

- Platform Support and Requirements for CA Process Automation Components (see page 26).
- Hardware Requirements (see page 28).

Follow these steps:

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

2. Verify that the host for the Domain Orchestrator has a supported JDK

   See JDK Prerequisites (see page 93).

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

   See Planning the Locations of Supporting Components (see page 85).

4. Identify the database server(s) to host the databases for the Library, Reporting, and Runtime data stores for the Domain Orchestrator.

5. Prepare the databases.

   See Database Server Prerequisites (see page 86).

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

7. Evaluate configuration options for CA EEM.

   See CA EEM Prerequisites (see page 95), including Prerequisites for Configuring NTLM Authentication.

8. If CA EEM is configured with CA SiteMinder, consider configuring CA Process Automation to use the SSO capability.

   See Using CA SiteMinder with CA Process Automation (see page 229).

9. Optionally, set up a load balancer if you anticipate the need to cluster the Domain Orchestrator at a later time. See Setting Up a Load Balancer for Orchestrator Clustering (see page 31).

10. Record, in a secure location, the certificate password that you plan to set in the Certificate Password field for the Domain Orchestrator.

    Important! You must provide this same password when you install other Orchestrators or additional Orchestrator nodes. If you forget this password, you will need to reinstall every Orchestrator in your system beginning with the Domain Orchestrator. This same password is required when you upgrade to a new release.

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 host with the CA Process Automation Domain Orchestrator and which ones to install on separate hosts. 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
- Databases for the CA Process Automation data stores - 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
- CA SiteMinder (optional) - can be colocated, but not recommended

Each cluster node and each Orchestrator is typically installed on a separate host. 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 host on which you installed the Domain Orchestrator:

- CA EEM.
- Database for the Library, Reports, and Runtime data stores.

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

- Characteristics of the host

  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 with the Domain Orchestrator. The only sure way to determine when you have enough resources is by actual full load testing.

Database Prerequisites

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

- MySQL r5.5
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Oracle Database 10g Release 2
- Oracle Database 11g Release 2

CA Process Automation has three data stores. Each of these data stores can reside in the same database, in different databases of the same type, or in databases of different types on the same or different database servers.

If you do not already have one of these databases, refer to the prerequisites for each before obtaining one. We recommend that this database and CA Process Automation reside on separate hosts.

Follow the guidelines for the type of database you are using for this Orchestrator installation.

- Prepare a MySQL Database for CA Process Automation (see page 88).
- Prepare a Microsoft SQL Server Database for CA Process Automation (see page 89).
- Prepare an Oracle Database for CA Process Automation (see page 91).

About CA Process Automation Data Stores

Each Orchestrator requires three logical data stores:

- The Repository data store, or *Library data store*, is a data store 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 data store on the Domain Orchestrator or each Orchestrator can have its own.

- The *Runtime data store* is an Orchestrator-specific data store that stores process instance data for a single Orchestrator or Orchestrator cluster. 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 standalone Orchestrator requires a separate Runtime data store. Because an Orchestrator cluster is seen as a single logical Orchestrator, all nodes share the same Runtime data store.

- The *Reporting data store* stores historical data for process and operator instances. 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 data store is typically shared among all Orchestrators.

The CA Process Automation data stores can share a physical database, but the best practice is to have a separate database for each data store. CA Process Automation requires database names to be case insensitive.

We recommend 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.

Archiving policy considerations

- Runtime data stores grow as processes are run, and the space required to store this data depends on the process instance content size as well as the CA Process Automation archiving policy settings.
- Process instances are stored based on the archiving policy. You can configure the archive purging policy to:
  - Move instances to the archive after a period of time.
  - Delete older instances automatically without moving them to the archive.
  - Take no action.

    Note: When the policy is set to take no action, we recommend that you perform data archiving tasks outside of CA Process Automation.
- The archiving policy is Orchestrator-specific.

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

More information:

Advanced Configuration Options (see page 22)

Prepare a MySQL Database for CA Process Automation

During installation of the Domain Orchestrator or an additional Orchestrator, the installer creates one or more databases. The databases are created in the specified MySQL database instances to house the CA Process Automation data stores. The installer requires the following prerequisites:

- The availability of MySQL JDBC driver version 5.1.7 or above.

  Note: This driver is not included in the CA Process Automation installation media.
- User credentials with Administrative privileges to create one or more databases for the Library, Reporting, and Runtime data stores.
- Two MySQL variables that are customized for CA Process Automation.

Before you install an Orchestrator that uses a MySQL database for CA Process Automation data stores, prepare the MySQL database.

Follow these steps:

1. Download the JDBC driver from the MySQL website. For example, get the MySQL Connector/J 5.1.7.
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. Set the maximum packet length to 33554432 Bytes (32 MB) 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 the required value.
6. Click Apply.

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

Prepare a Microsoft SQL Server Database for CA Process Automation

Before installing the CA Process Automation Domain Orchestrator or an additional Orchestrator, where the CA Process Automation data stores reside on one or more SQL Server databases, make the following preparations:

- Verify that the SQL Server meets CA Process Automation requirements (see page 90).
- Understand how the JDBC 3.0 driver is referenced (see page 90).
- Review the guidelines for specifying the Database Server name for SQL Server (see page 91).

Verify that the SQL Server Database Meets CA Process Automation Requirements

The SQL Server that you prepare for CA Process Automation data stores 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 databases for the CA Process Automation data stores.
- SQL Server collation must be SQL_Latin1_General_CP1_CI_AS for databases that hold the CA Process Automation data stores. 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 JTDS JDBC Driver Is Referenced

During installation of the Orchestrator, the installer requires the JTDS 1.3 driver for SQL Server, which is included in DVD1. The path is:

```
.../DVD1/drivers/jtds-1.3.jar
```

Guidelines for Specifying the Database Server Name for a SQL Server Database

When you install the Domain Orchestrator or any nonclustered Orchestrator, you specify details for three CA Process Automation data stores: Library, Runtime, and Reporting. If you define the Type of Database as MS SQL, use the following guidelines to specify the Database Server:

- If you have only one SQL Server instance on the host server, specify the host name of the server. (This name is the default instance.)
- If you have multiple SQL Server instances on the host server, specify the SQL Server named instance in the format *host_name**named_instance*.

  A SQL Server named instance is another copy of SQL Server running on the same host. Each copy runs independently; each copy is distinguished by its instance name. A database server can have many named instances but only one default (unnamed) instance.

Prepare an Oracle Database for CA Process Automation

Before you install the Domain Orchestrator or an additional Orchestrator, which uses one or more Oracle databases to host its data stores, preparation is required.

Follow these steps:

1. Open an Oracle database management application and log into the target Oracle database instance.
2. Create a schema for each of the following data stores, where each schema has the permissions listed in Database Owner Privileges (see page 92).
   - Library data store
   - Runtime data store
   - Reporting data store
3. Verify that Oracle has sufficient tablespace to host the data stores.

   Note: See About CA Process Automation Data Stores (see page 87) for more information about space considerations.

4. 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.

5. Follow Online Transaction Processing (OLTP) best practices to facilitate CA Process Automation transactions.

6. Understand how the Oracle JDBC driver is referenced.

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

   ```
   .../DVD1/drivers/ojdbc14.jar
   ```

Note: Partitioning is *not* supported.

More information:

Oracle Bug # 9347941 (see page 265)
Change the Database Configuration to Use an Oracle Service Name (see page 148)

Database Owner Privileges

When you start CA Process Automation for the first time or when you apply a patch, the application adjusts the database or schema structure.

To adjust the structure, CA Process Automation requires the following database privileges at a minimum:

- The right to access metadata (to determine the structure)
- The right to CAD (create/alter/drop) tables, indexes, views, constraints, and sequences in the database.
- Read or Write rights on all its tables

CA Process Automation requires the following privileges for its tables during runtime:

- Select
- Insert
- Update
- Delete

JDK Prerequisites

Before you install any Orchestrator, verify that the Java Development Kit (JDK) prerequisites are met. Use the following command:

```
Java –version
```

```
C:\>Java -version
java version "1.7.0_45"
Java(TM) SE Runtime Environment (build 1.7.0_45-b18)
Java HotSpot(TM) 64-Bit Server VM (build 24.45-b08, mixed mode)
```

The preceding example shows a valid Java version for Windows.

Follow these steps:

1. Log in to host where you plan to install the Domain Orchestrator.
2. Verify that your Java Development Kit is Oracle JDK 1.7.

   Note: For other details, see Platform Support and Requirements for CA Process Automation Components (see page 26). If default Java version is different, change the default Java version on the shell where you will start the CA Process Automation installer.
3. If the required JDK version is not installed, download it from the Oracle website and run the installation wizard to install the JDK.
4. For a clustered Orchestrator, ensure that Oracle JDK is installed on each node.

Setting the Default Java Home Path

If the default version is different, change the default Java version on the shell where you will start the CA Process Automation installation.

Follow these steps:

1. Browse to DVD1 folder
2. Set default java on the command prompt or shell.

   Windows

   ```
   set JAVA_HOME=<home_directory_of_jdk (not_bin)>
   set PATH=%JAVA_HOME%\bin;%PATH%
   ```

   UNIX or Linux

   ```
   export JAVA_HOME=<home_directory_of_jdk (not_bin)>
   export PATH=$JAVA_HOME/bin:$PATH
   ```

3. Start the installer from this command prompt or shell.

   Windows

   ```
   .\ Domain_Installer_windows.bat
   ```

   UNIX or Linux

   ```
   ./ Domain_Installer_unix.sh
   ```

   The installer first starts the third-party installer and then starts the Domain Orchestrator installer.

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, verify that it is a version supported by CA Process Automation. See Platform Support and Requirements for CA Process Automation Components (see page 26).
- 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 96).
- Plan how to authenticate CA Process Automation users (see page 102).
- Gather CA EEM related information for the Domain Orchestrator installation (see page 98).
- 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 97). This procedure is optional and can be performed at a later time.

Note: For CA EEM-specific details, click one of the CA Process Automation bookshelf links in the Product Documentation - CA Embedded Entitlements Manager area, which includes the CA Embedded Entitlements Manager *Integration Deployment Guide*.

Set Up CA EEM

CA Process Automation requires CA EEM to manage authorization to the CA Process Automation UI. A suitable CA EEM instance must be available prior to installing or upgrading CA Process Automation. CA Process Automation can use any version of CA EEM from 8.4 SP04 CR10 through 12.51, but certain CA EEM features that CA Process Automation can use are not supported in all CA EEM versions. For example:

- Support of 2048- and 4096-bit security certificates requires CA EEM Release 12.5 or later (English) and Release 12.51 (other supported languages).
- Support of multiple Microsoft Active Directory Domains requires CA EEM version 12.0 or later.
- If your site has an existing CA EEM instance that is not at the required version, consult with your site administrator to see if the CA EEM instance can be upgraded to the desired level. Version support limitations for other products using the CA EEM instance can preclude upgrading the instance.

New CA EEM Installation

A new CA EEM installation is required if no CA EEM instance at the desired version is available.

Follow these steps:

1. Download installers for CA EEM 12.51 from the CA Support Online.
2. Follow the instructions provided in the CA EEM documentation when deploying or upgrading your CA EEM instance.

CA EEM Configuration Considerations

- When you configure CA EEM to use the internal user store or an external user store, consider the following implications for CA Process Automation:
  - If you select the default internal user store, you create user accounts for CA Process Automation users. User credentials defined in CA EEM are used for authentication at login.
  - If you point to an external user store, then user accounts from that store are loaded into CA EEM as global users. User credentials defined in the referenced LDAP-based directory are used for authentication.

    See Reference Global Users and Global Groups from Microsoft Active Directory (see page 106). (CA EEM 8.4)

    See Reference Global Users from Multiple Active Directories (see page 106). (CA EEM 12.51)
  - If your CA EEM is configured to use multiple active directories, verify that the ID of the person who who installs or upgrades CA Process Automation is included in each of the referenced active directories.

Important! If absent, add your administrator ID to each referenced Active Directory before installing or upgrading CA Process Automation. You use this ID to test connectivity between CA Process Automation and CA EEM during installation or upgrade.

- When you configure CA EEM to use FIPS mode, CA Process Automation must be configured to use FIPS-compliant algorithms for communication between CA Process Automation and CA EEM. During CA Process Automation installation, you select Use FIPS-Compliant Certificate to use FIPS-compliant algorithms. CA Process Automation and CA EEM encrypt the data that is transported between them using a FIPS-compliant algorithm.

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 authentication and authorization server for CA Process Automation. The secondary CA EEM is the standby security authentication and 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).

Gather CA EEM Related Information for the Domain Orchestrator Installation

Before you begin the installation of the Domain Orchestrator, have at hand the following details of your CA EEM configuration:

- The CA EEM administrator credentials, where EiamAdmin is the user name.
- The CA EEM release version and the FIPS setting in CA EEM.

  1. Browse to the CA EEM you are using.

     `https://server:5250/spin/eiam`

  2. Select the CA Process Automation application name from the Application drop-down list.
  3. Enter valid login credentials, for example, **EiamAdmin** and the associated password. Click Login.
  4. Click About. The CA EEM release version and the FIPS setting appear under Product Specifications.

Note: During the CA Process Automation installation, the process that registers the CA Process Automation application with CA EEM also generates the certificates that CA Process Automation uses to connect to CA EEM.

- If CA EEM is FIPS-enabled, then the PAM.cer and PAM.key are both generated.
- If CA EEM is FIPS-disabled, then you provide a password (the EEM Certificate password) before registering the CA Process Automation application in with CA EEM. This password is then used to protect the PAM.p12 certificate that gets generated when registering the CA Process Automation application with CA EEM.
- If you install *without registering* the CA Process Automation application with CA EEM, you are prompted to select the SDK corresponding to your CA EEM server version.

- The host name of the CA EEM server. To determine the host name, log in to CA EEM. The host name is displayed with the label, Backend, in the title bar.

  Important! You need the EiamAdmin password to log in to CA EEM.

- If you are upgrading and plan to configure CA EEM to use multiple Microsoft Active Directories, know the name of the AD domain that you currently reference. Consider specifying this domain as the default AD domain. CA Process Automation users belonging to the default AD domain can log in to CA Process Automation with their unqualified user name after you reassign them to an application group.
- Record the certificate password that you plan to enter. This certificate password controls access to the keys that encrypt passwords and other critical data. The certificate password is specific to a single CA Process Automation Domain. (This certificate password is not CA EEM-related, but it is important to record it.)

  Important! You must use this same password when you install any other Orchestrator or when you add cluster nodes to an Orchestrator. This same password is a required entry when you upgrade CA Process Automation.

Identify the Version of the CA EEM SDK that CA Process Automation Uses

You can determine whether the CA EEM SDK that CA Process Automation uses is SDK Version 8 or SDK Version 12.

Follow these steps:

1. Stop the Domain Orchestrator
2. Increase the log level of the Domain Orchestrator to INFO.
3. Start the Domain Orchestrator.
4. Log in to the CA Process Automation server.
5. Review the logs.
   - If CA Process Automation is using CA EEM SDK r8.4:

     ```
     13:03:16,859 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByUserName in class:
     com.ca.eiam.SafeGlobalUser. The current EEM SDK's version is
     8
     13:03:16,861 INFO
     [com.optinuity.c2o.eemconfiguration.EEM8Manager]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM8Manager...
     ```

   - If CA Process Automation is using CA EEM SDK 12.51:

     ```
     13:32:37,195 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByPrincipalName in class:
     com.ca.eiam.SafeGlobalUser. The current EEM SDK's version is
     12
     13:32:37,198 INFO
     [com.optinuity.c2o.eemconfiguration.EEM12Manager]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM12Manager...
     ```

6. Stop the Domain Orchestrator, return the log level setting to the previous level, and then restart the Domain Orchestrator.

Prerequisites for Configuring NTLM Authentication

Do the following before your configure NTLM authentication:

- Verify that CA EEM is installed on a server with a Microsoft Windows operating system.
- Verify that CA EEM uses Microsoft Active Directory as the external user store.
- Verify that CA EEM is not configured for Multiple Active Directories or for an Active Directory forest.
- Verify that users browse to CA Process Automation from a Windows computer.
- Verify that the CA EEM Server and the computer from which users browse to CA Process Automation are part of the same network domain. If the computers are part of nested domains, ensure that the CA EEM Server and the computer where the application is launched belong to domains that have a trust relationship established.
- Verify that the domain users are added to the User Groups on the computer where the application is being launched.

Plan How to Authenticate CA Process Automation Users

If this is a new CA Process Automation installation, part of preparation is determining how to authenticate CA Process Automation users. The actual setup described here is performed after installation is complete. However, the authentication method that is chosen determines the settings specified during the CA Process Automation installation. Authentication options include:

CA EEM-based Authentication

- Native CA EEM-based user

  Prerequisites

  Installation of CA EEM

  Details

  A CA EEM administrator creates a user account in CA EEM for each user who requires access to CA Process Automation. The CA EEM administrator provides each user with a login ID. Users can update their own passwords in CA EEM. When users log in to CA Process Automation, CA EEM authenticates users by verifying that the entered User ID and password (credentials) belong to an active user account.

  Action that is required during CA Process Automation installation

  No special action required.

- Reference to LDAP directory

  Prerequisites

  - Installation of CA EEM
  - Access to an external LDAP-based directory

  Details

  The following directory types and configurations are available:

  - Active Directory (AD)

    CA EEM can be configured to reference user accounts that are stored in one or more Microsoft Active Directories. CA Process Automation passes CA EEM the login credentials. CA EEM finds the AD that matches the domain part of the user ID (if relevant) and authenticates the user if the user ID is listed within that AD domain.

  - Non-AD LDAP-based directory

    CA EEM can also be configured to use an LDAP-based directory other than AD. Authentication is handled the same way in this case.

  Action that is required during CA Process Automation installation

  No special action required.

- Single Sign On using NTLM authentication

Prerequisites

- Same prerequisites as when using AD with the previous LDAP directory option.
- You must be able to meet the prerequisites for configuring NTLM authentication.

  Note: One of the requirements is that CA Process Automation users run a Windows operating system and be in the same Domain as, or in Domains with trusted relationships to, the CA EEM server.

Details

CA EEM handles authentication through NTLM when users browse to CA Process Automation. Authenticated users are logged in with their Windows credentials.

Action that is required during CA Process Automation installation

Select the NTLM option on the CA EEM wizard page during CA Process Automation installation. This is the recommended way to enable SSO.

Note: You can enable NTLM pass-through authentication after installation, if required.

SiteMinder-based Authentication

- Single Sign On using CA SiteMinder

Prerequisites

See the SiteMinder documentation for specific information.

Details

SiteMinder authenticates with an external directory and sends the user name to CA Process Automation. The user is then authorized in CA EEM. See Using SiteMinder with CA Process Automation (see page 229) for details.

Action that is required during CA Process Automation installation

SiteMinder hostname and headers are specified on load balancer wizard page.

User Authentication and Authorization in FIPS Mode

CA EEM can be configured to use FIPS mode. This is an option. When CA EEM is configured to use FIPS, CA Process Automation must be configured to use FIPS. This is achieved by selecting the Use FIPS-Compliant Certificate check box during installation of the Domain Orchestrator.

Whether FIPS mode is set to on or off, the data transferred between CA EEM and CA Process Automation is encrypted. The difference is in the algorithms used for encryption.

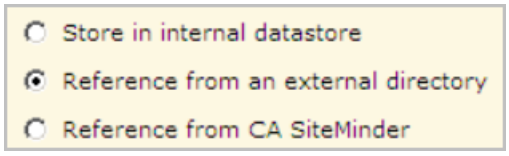
When users log in, CA Process Automation transfers the user name and password to CA EEM. CA EEM returns authentication data and authorization data to CA Process Automation.

- When FIPS mode is on:
  - Transferred data is encrypted with the SHA1 algorithm supported by FIPS.
  - A PAM.cer certificate is used.
- When FIPS mode is off:
  - Transferred data is encrypted with the MD5 algorithm.
  - A PAM.p12 certificate is used.

Define the CA EEM Configuration Type for Storing Global Users

If you are completing CA EEM prerequisites for the initial installation of CA Process Automation, consider the following:

- Part of CA EEM configuration is selecting whether to store user credentials internally or reference user credentials from an external directory or from SiteMinder.



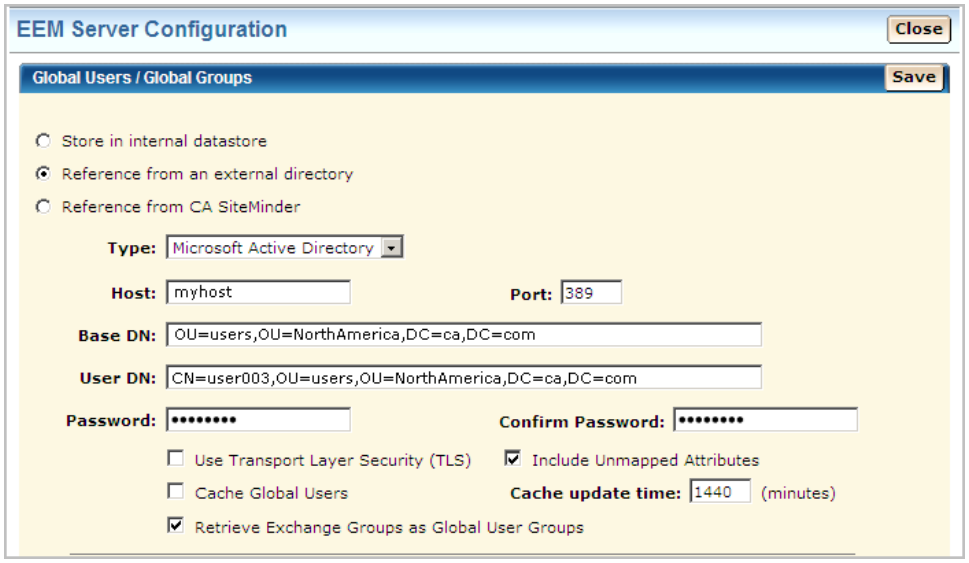
- If you are using an existing CA EEM that supports applications other than CA Process Automation, this option and the configuration type is already defined. All applications use the same configuration type. Configuration types vary by release.
  - The CA EEM Release 8.4 "Reference from an external directory" option includes the configuration type Microsoft Active Directory
  - The CA EEM Release 12.5 "Reference from an external directory" option includes its own set of configuration types, including multiple AD domains and an AD forest.
- If you are using a new CA EEM instance, consider using this procedure:
  1. Install CA EEM and start CA EEM.
  2. Install CA Process Automation. During installation, register with CA EEM which creates the CA Process Automation application in CA EEM, and skip the test for connectivity to CA EEM.
  3. Log into CA EEM with the EiamAdmin user credentials and the CA Process Automation application name.
  4. Define the user store, and if you select Reference from an external directory, define the details.

     For more information about configuring Global Users from a referenced user store in CA EEM, see the CA EEM documentation. See also the following examples:
     - Reference Global Users and Global Groups from Microsoft Active Directory (see page 106) (CA EEM r8.4).
     - Reference Global Users from Multiple Active Directories (CA EEM r12.5) (see page 106)
  5. While in CA EEM, configure CA Process Automation users. See "Assign an Application Group to a Global User" in the *Content Administrator Guide*.
  6. Optionally, configure CA EEM to permit referenced users to log in with their email names (see page 145).

Reference Global Users from a Microsoft Active Directory (CA EEM r8.4)

While you are installing CA EEM r8.4, you can select the Reference from an External Directory option and then select Microsoft Active Directory as the type.

When you use NTLM for security, select the Retrieve Exchange Groups as Global User Groups check box as in the following example:



When you save the configuration, the following status messages appear:

- External directory bind succeeded.
- External directory data is loaded.

If NTLM is enabled and a global user logs in for the first time, an Authentication Required dialog opens. CA EEM then uses the NTLM protocol to authenticate users.

Reference Global Users from Multiple Active Directories (CA EEM 12.5)

While you are installing CA EEM r12.51, you can configure CA EEM to reference multiple Microsoft Active Directories or an Active Directory forest.

Follow these steps:

1. Log in to CA EEM as the EiamAdmin user. Specify <Global> as the application.
2. Click the Configure tab, then click User Store.
3. Select User Store from the User Store palette.
4. For Global Users / Global Groups, select Reference from an external LDAP Directory.

5. Select Multiple Microsoft Active Directory Domains from the Configuration Type drop-down list.
6. Click Add Directory and enter the first Active Directory name in the Name field.
7. Under Domain Settings, enter the domain in the Domain field.
8. Enter the host name and the port number in the Host and Port fields, and then click the right arrow.

   The Selected Hostnames list specifies where the Active Directory is located.
9. Select the protocol you need from the Protocol drop-down list.
10. For Base DN (Base Distinguished Name), enter a value without spaces. The value specifies the external LDAP directory that contains data for global users and global groups. In the following example, the OU= value limits the global groups that are loaded to those in the specified organizational unit.

    ```
    OU=myorganizationalunit,DC=foo,DC=com
    ```
11. Specify the credentials that CA EEM is to use to access the specified Domain and Organizational Unit. This user must be a member of the Domain and the Organizational Unit specified for the Base DN.
    a. For User DN (User Distinguished Name), enter the Common Name of the user to connect to the external LDAP directory. Use the escape character (\) before a comma between parts of the common name. For example

       ```
       CN=firstname\,lastname,DC=foo,DC=com
       ```
    b. Enter the password associated with the common name specified for User DN for User Password and for Confirm Password.
12. Complete the Advanced Configuration or accept the defaults.
13. Repeat Steps 6 through 12 for each AD to reference.
14. Click Save.

    When you save the configuration, the following status messages appear:

    - External directory bind succeeded.
    - External directory data is loaded.

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 ports in Ports Used by CA Process Automation (see page 235) and plan for substitutions for any ports 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.

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.

If you have a load balancer, we recommend that you set up the Domain Orchestrator as a clustered Orchestrator, even if you have no plans to cluster at the present time. If you decide to cluster later and have not set up the Domain Orchestrator as clustered, you must reinstall the Domain Orchestrator to support clustering. For details, see:

- NGINX Load Balancer Prerequisites (see page 64).
- F5 Load Balancer Prerequisites (see page 52).
- Apache Load Balancer Prerequisites (see page 32).

Subsequent installations require certain values that you configure during Domain Orchestrator installation. For example, certain passwords must be reentered during upgrade or installation of 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 specific passwords.

- CA Process Automation certificate.
- CA EEM certificate.
- Repository data store.
- Reporting data store.
- Runtime data store.
- CA EEM administrator.

More information:

Unattended Domain Orchestrator Installation (see page 131)

Install the Third-Party Software

You begin the CA Process Automation installation by installing the third-party software. When this installation completes, the Orchestrator installation begins automatically.

Follow these steps:

1. Insert DVD1 of the CA Process Automation installation media into a drive. Alternatively, browse to the location where the DVD1 and DVD2 folders containing the installation files were copied.

   Note: In Red Hat Enterprise Linux, to execute permissions on the .sh file, enable the execute permissions on the .sh files. For example, execute permission on the .sh files using the following commands:

   ```
   chmod a+x Domain_Installer_unix.sh
   chmod a+x Third_Party_Installer_unix.sh
   ```

2. Run the installation program appropriate to your platform and media:

   - **Windows:** Domain_Installer_windows.bat
   - **Linux or UNIX:** Domain_Installer_unix.sh

   These files invoke the third-party installer and then the Domain Orchestrator installer.

3. Select the preferred language from the Language Selection dialog.

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

   The Welcome to the CA Process Automation third-party Installer Setup Wizard appears.

4. Click Next to begin the 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.

   If the destination folder does not exist, the installer creates the folder. 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 recommend keeping the installation path (*install_dir*) to 64 characters or less.

   The list of third-party prerequisites appears. Third-party pre-requisites for the Domain Orchestrator include JBoss Installation, Hibernate Installation, and JDBC Jar Installation. In CA Process Automation r 4.2, the ActiveMQ messaging service is used with JBoss 5.1.

7. Click Next and then monitor the installation of JBoss and third-party components.

   The JDBC Jars Installation appears.

8. Select one or more database applications to host CA Process Automation data stores 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 JTDS JDBC jar file on DVD1 installation disk. For example:

     `...\DVD1\drivers\jtds-1.3.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 Orchestrator 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 replace DVD1 with DVD2 in the field. (Alternatively, 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

After the Third-Party Installer installs third-party components, the Third-Party installation wizard starts the Domain Orchestrator installation wizard.

This section describes how to install a nonclustered Domain Orchestrator or the first node of a clustered Domain Orchestrator.

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 the path to the Java Home Directory is not displayed, complete the following steps:
   a. Click Browse
   b. Navigate to the correct location
   c. Select the Java Development Kit (JDK) to use. For example, select:

      ```
      C:\Program Files\Java\jdk1.7.0_21
      ```

   d. Click Next.

   The JDK is validated.
4. Monitor the progress as files are copied.
5. For CA Process Automation Domain Configuration, specify the following, which applies to all components:
   - Domain Orchestrator
   - Load balancer, if the Domain Orchestrator is a clustered Orchestrator
   - CA SiteMinder SPS, if configured

   Support Secure Communication

   Specifies whether the relevant components communicate over HTTPS (secure) or HTTP (basic).

   Selected

   Indicates that the entire communication channel is secure (uses HTTPS to communicate).

   Cleared

   Indicates that the entire communication channel uses HTTP to communicate.
6. To configure CA Process Automation for use with CA SiteMinder Secure Proxy Server (CA SiteMinder SPS), verify that all CA SiteMinder SPS prerequisites are met. Then, complete the following fields on the CA Process Automation Domain Configuration screen:

   Configure CA SiteMinder Single Sign-on (SSO)

   Select this check box to configure CA SiteMinder SPS with the Domain Orchestrator.

   Secure Proxy Server Host

   Defines a FQDN hostname of CA SiteMinder SPS.

Secure Proxy Sever Port

Defines the port number of CA SiteMinder SPS.

Type of Server

Specifies the type of installation as New Orchestrator.

7. Read the instructions and complete the Configuration Screen.

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. Before you select this option, verify that you have completed the NGINX Load Balancer (see page 63) prerequisites or the F5 Load Balancer Prerequisites (see page 52).

Cleared

Install the Domain Orchestrator with no potential for clustering.

Load Balancer Worker Node

Defines the name of the Load Balancer Worker Node. Because the first installation of the Domain Orchestrator is the first node in the cluster, this value is typically node1.

If Apache is your load balancer, your entry must match the node name in the "worker.*nodename*.host" variable that is associated with this host in the Apache file *apache_install_dir*\conf\workers.properties. In the following example, the variable value, **node1**, is the value to assign here.

`worker.`**`node1`**`.host=`*`DomainOrchestratorHostName`*

If the workers.properties file specified worker.**abc**.host, then you would enter **abc**.

If F5 is your load balancer, accept the default. (The value of the worker nodes is not relevant to F5, so there is no tie-back to the F5 prerequisites that you performed.)

Default: node1 (Special characters, including dashes, are not supported.)

Public Host Name

Specifies the public host name for the Apache server, NGINX server, or the F5 server. For example:

`loadbalancerhost.mycompany``.com`

- Set this field to the FQDN of the Apache, F5, or NGINX load balancer if you selected the Configure Load Balancer check box.

Public Host Port Number

Defines the HTTP port for the Load Balancer.

If you change this value during the Apache, F5, or NGINX Load Balancer installation and configuration, update this value accordingly. This port is used with the Public Host Name value to browse to CA Process Automation. For example:

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

Default: 80

Public Host Secure Port

Defines the HTTPS port for the Load Balancer.

This port is used with the Public Host Name value to browse to CA Process Automation. For example:

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

Default: 443

8. Click Next.
9. In the Company field, type your company name, and then click Next.

   CA Process Automation displays your entry as the This Product is Licensed To value when you click Help, About.
10. Type a certificate password, type it again, and then click Next.

    Certificate Password

    Defines the password that controls access to the keys that encrypt passwords and other critical data. Use this same password when you install any other Orchestrator or when you add cluster nodes to an Orchestrator. The certificate password is specific to a single CA Process Automation Domain.

    Confirm Certificate Password

    Matches your entry in this field with your entry in the Certificate Password field to verify the password.

    Important! In the Set Certificate Password page, before you click Next, record your Certificate Password entry in a secure location for later reference. This same certificate password is required when you install standalone Orchestrators or when you add cluster nodes.

11. (Windows only) Specify the following Start Menu preferences, then click Next.

    [Start menu folder name]

    Defines the name of the CA Process Automation Start menu folder if you cleared the Do Not Create a Start Menu Folder check box. Accept the default or type the name of the Start menu folder for CA Process Automation.

    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 in 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 a Start menu entry for CA Process Automation.

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

12. Complete the following fields to define how the Domain Orchestrator communicates with other CA Process Automation components and applications, then click Next.

    Server Host

    Defines one of the following properties:

    - The host name or IP address of the host system on which the Domain Orchestrator is deployed.
    - A DNS Alias that resolves to the host system.

    Display Name

    Defines the Domain Orchestrator name that appears 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 on which the load balancer is installed.

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. Use HTTP instead.

Server Port

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

Default: 80 (basic: HTTP), or 443 (secured: HTTPS)

HTTP Port

Defines the HTTP port that is used for the web server if the Support Secure Communication check box is cleared.

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

Default: 8080

HTTPS Port

When you select Support Secure Communication, this field specifies the port used in the URL that accesses CA Process Automation Web services and the browser-based CA Process Automation UI.

Default: 8443

Note: Select “Support Secure Communication” to enable input to this field.

JNDI Port

Defines the Java naming server port that the web server uses.

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

Default: 1099

RMI Port

Defines the RMI port that the web server uses.

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

Default: 1098

SNMP Port

Defines the SNMP trap listener port for CA Process Automation.

Default: 162

13. Accept the default path or browse to a temporary directory in which to run scripts. Click Next.

    This directory must be writable by all users.

14. Complete the following fields to define PowerShell settings, then click Next.

    Set PowerShell Execution Policy

    Specifies whether to enable the use of PowerShell.

    Selected: Enable the use of PowerShell, setting the PowerShell execution policy at the specified path to Remote Signed.

    Cleared: Do not enable the use of PowerShell.

    PowerShell Path on host machine

    CA Process Automation auto-detects the PowerShell path.

    Note: When you click Next, the installation program validates the provided PowerShell path.

15. Define the CA EEM security settings. The order in which fields are presented in this step is based on dependencies rather than the field order displayed in the UI.

    a. Complete the following required fields:

    EEM Server

    Defines the FQDN of the CA EEM server that CA Process Automation uses to authenticate and authorize CA Process Automation users. If you are configuring EEM for High Availability (HA), you can also define a backup CA EEM server. Use a comma as the delimiter between the server names.

    EEM Application Name

    Defines how the CA Process Automation application name appears in CA EEM. If you use the same CA EEM server with multiple CA Process Automation Domains, each CA Process Automation domain must have a unique EEM application name. The name that you enter here appears in the drop-down list of the CA EEM server login page.

    If you are upgrading, this field is already populated with the value used in the initial installation. This value preserves the CA EEM user group assignments, custom policies, and custom groups. CA EEM uses this value to identify this CA Process Automation domain.

    Default: Process Automation

    Use FIPS-Compliant Certificate

    Specifies whether to use FIPS-compliant certificates. This setting must match the CA EEM setting for FIPS Mode.

    Note: To determine the CA EEM setting for FIPS, click About in CA EEM; the Product Specifications include FIPS Disabled or FIPS Enabled.

    Selected: FIPS Mode is set to ON in CA EEM.

    Cleared: FIPS Mode is set to OFF in CA EEM.

b. Specify your *intent to register* the specified application name for this CA Process Automation domain with CA EEM after completing this page. The registration process generates either FIPS-compliant certificates or non-FIPS compliant certificates, based on your selection. This check box appears above the Register button. Selection is the typical configuration.

Register Application with CA EEM

Specifies whether to register the "EEM Application Name" value for CA Process Automation with CA EEM and generate the certificate that CA Process Automation uses to connect to its application in the CA EEM server. The CA EEM SDK handles the connection. If prompted, indicate that you want to upgrade the CA Process Automation application in CA EEM.

Selected: Enables the Register button. (See Step 16.) Disables the EEM Certificate File field. For a new installation of a Domain Orchestrator, always select this check box. When you complete the EEM Security Settings fields, click Register.

Cleared: Disables the Register button. Enables the EEM Certificate File field.

c. For a new installation, complete the following field only if you are not registering the application with CA EEM. Click Browse and find the location of the Certificate file. Once the certificate file uploads, the installer places it in this directory:

`install_dir/server/c2o/.c2orepository/public/certification`

Note: If you are upgrading, this field is automatically populated with the path to your certificate file.

EEM Certificate File

Defines the CA EEM certificate file to use for CA Process Automation. You can typically accept the default value.

Defaults:

PAM.cer if you selected the Use FIPS-Compliant Certificate check box.

PAM.p12 if you cleared the Use FIPS-Compliant Certificate check box.

d. Complete one of the following fields, if required.

Certificate Key File

If required (see Notes), click Browse and find the location of the certificate key, for example, the PAM.key file. Once the certificate file uploads, the installer places it in this directory:

install_dir/server/c2o/.c2orepository/public/certification

Notes:

- If this is a new installation, this field is not required if you are using FIPS and you intend to register. (The registration process generates the certificate key file with the certificate.)
- If this is a new installation, this field is required if you are using FIPS and you do not intend to register.
- If you are upgrading, this field is populated with the path to your key file.

EEM Certificate Password

Required if you are not using FIPS. Defines the CA EEM Certificate password. This password protects the PAM.p12 certificate; CA Process Automation needs this password to open and use the PAM.p12 certificate.

e. Complete the following fields only if you configure CA EEM to reference users from an external LDAP directory. Otherwise, skip this step.

Default Active Directory Domain

(Applicable only if you plan to reference multiple Active Directory domains when you configure CA EEM Release 12.51. See Step 17.) Specifies the AD domain to use as the default domain. CA Process Automation users belonging to the domain specified here can log in to CA Process Automation with their unqualified user name. Users belonging to other AD domains must specify their principal name (*domain**username* or *username*@*domain*) and password when they log in to CA Process Automation. This entry must match the Domain field entry for one of the multiple AD domains you configure for the CA EEM referenced user store.

CA EEM must be suitably configured to authenticate with the username@domain form of the principal name.

Note: See Configure CA EEM to Permit Referenced Users to Log in with Their Email Name (see page 145).

Enable NTLM Pass-Through Authentication

Specifies whether CA EEM uses the NTLM protocol to authenticate CA Process Automation users.

Selected: Enables NTLM pass-through authentication. CA EEM uses the NTLM protocol to authenticate users who browse to CA Process Automation.

Cleared: Disables NTLM pass-through authentication. Users who browse to CA Process Automation must enter credentials in the CA Process Automation login dialog. CA EEM validates the credentials with the referenced Microsoft Active Directories to authenticates users.

16. Either register the configured "EEM Application Name" value with CA EEM or bypass registration. The registration process generates CA Process Automation certificates of the required length.

    - If this is a new installation, click Register, complete the following fields on the EEM Credentials window and click OK. Click OK when the Application Registered confirmation appears.

      EEM Admin Username

      Defines the CA EEM administrator user name. Type **EiamAdmin**.

      EEM Admin Password

      Defines the password for the EiamAdmin user account. If you installed CA EEM, enter the password that you created for the EiamAdmin user. Otherwise, contact the CA EEM administrator to get the password.

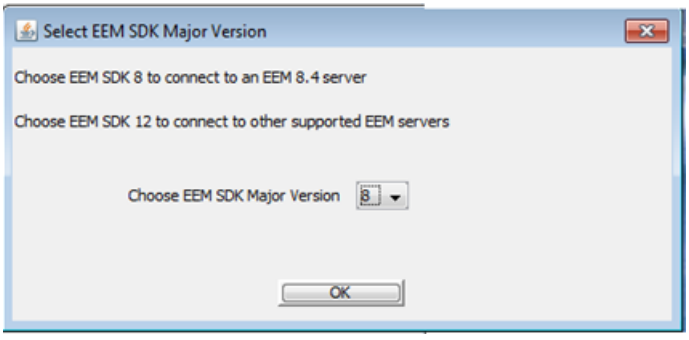
    - If using FIPS certificates, new 'PAM.cer' and 'PAM.key' certificates overwrite the existing certificates, if any. If not using FIPS certificates, the new PAM.p12 overwrites the existing certificate in CA Process Automation, if it exists. This certificate is password-protected with the password you entered in the EEM Certificate Password field. The EEM Certificate File is populated with a path and file name similar to this example:

      install_dir`/server/c2o/.c2orepository/public/certification/PAM.p12`

      Note: The certificates are not regenerated if you are prompted to upgrade the CA Process Automation application in CA Embedded Entitlements Manager, and you choose *not* to upgrade it.

    The following bulleted list describes the use cases:

    - New Installation with Registration: The installation process detects the CA EEM server version and choses the appropriate SDK.
    - New Installation without Registration: The installation process prompts you to choose an SDK based on the CA EEM release version. If you do not know the release version of the CA EEM server, log in to CA EEM and review the About information.

17. (Optional) If you want to test the CA EEM settings and you have configured CA EEM to reference from an external directory, you must first create a test user. A test user is a user you retrieve from a selected Active Directory and then assign to the PAMAdmins group. Follow these steps:

    a. Browse to the CA EEM that CA Process Automation uses. Use the following URL:

       `https://hostname:5250/spin/eiam`

       The CA Embedded Entitlements Manager dialog opens.

    b. From the Application drop-down list, select the name you configured in the EEM Application name field.

    c. Type EiamAdmin and the CA EEM administrator password that you configured.

    d. Click Log In.

    e. Click the Manage Identities tab.

    f. Under Search Users, where Global Users is selected, select Last Name or First Name and enter your first or last name in the Value field. Then, click Go. (Partial values are accepted.)

       Your name appears under Users in the Users pane.

    g. Double-click your name to display your loaded user account.

       Your user account has two User Details sections. The top section lets you define a group for your role in CA Process Automation. The bottom section, "Global User Details" contains information from the external directory.

    h. Click the Add Application User Details button under the top section.

       The Available User Groups list contains a group for each default role.

    i. Select PAMAdmins and click the right arrow to move that group to the Selected User Groups list.

    j. Click Save.

    k. Click Log Out.

18. (Optional) Test the CA EEM settings. This step requires you to enter the credentials of a user that is defined in CA EEM. If you are using CA EEM as a local directory (the default), you can enter credentials of one of the default users. If CA EEM points to an external directory, you enter your own credentials (if you completed the preceding step).

    a. Click Test CA EEM Settings.

    b. If using CA EEM as a local directory and this is a new installation, type pamadmin for Username, type pamadmin for Password, and click OK.

    c. If using a referenced user account from an external directory, type your user credentials as defined in the external directory. This is the account of the test user that you created in the preceding step.

    The Verify EEM Settings screen displays the following fields:

    Connect

    Indicates whether a connection can be established to the specified CA EEM server with the values provided in the CA EEM settings screen.

    Limits: OK, NOT OK

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

    User provided belongs to User Group

    Indicates whether the user can be authenticated, that is, whether login is permitted.

    Limits: OK, NOT OK

    User is an Admin

    Indicates whether the user has authorization to perform administrator tasks. Members of the PAMAdmins group have this authorization.

    Limits: Yes, No

    EEM Upgrade

    Indicates whether the CA Process Automation application schema in the EEM server is upgraded. If the message "Upgrade not required" appears; click OK.

    Note: This field is displayed only when the value is NOT OK. When the value is NOT OK, upgrade the instance.

19. After you review the results, click OK, then click Next.

20. Complete the following fields to define the database that is to host the Library data store and the database server on which the database is installed.

Type of Database

Specifies the Database system type. Select a supported type from the drop-down list.

Values: MySQL, MS SQL, Oracle

Note: If this installation is for production use, best practice is to select either MS SQL or Oracle. MySQL is an appropriate choice for a lightly-loaded Domain Orchestrator.

User Name

For MS SQL and MySQL, defines a user name that is 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. The following values are auto-populated based on the database selection:

- MS SQL: **sa**
- MySQL: **root**

For Oracle, defines an existing schema that is authorized to create and access the CA Process Automation database objects.

Password

Defines the password that is associated with the specified User Name.

Database Server

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

- If you configured the Type of Database as MS SQL and you have only one SQL Server instance on the host server or if you selected another database type, specify the host name or IP address of the database server. (This entry refers to the default instance.)
- If you configured the Type of Database as MS SQL and you have multiple SQL Server instances on the host server, specify the SQL Server named instance. Use the format host\instance, for example, *dbserver.mycompany*.com*pamdb.*

Database Port

Defines the connection port that is configured on the target database instance.

- For MS SQL, the default port is 1433.
- For MySQL, the default port is 3306.
- For Oracle, the default port is 1521.

Repository Database

Defines the name of the database in which to store Library objects and other data.

Each Orchestrator can have its own repository, or library, data store. You can also share the library data store across Orchestrators. Each data store must have a unique name. Consider establishing a naming convention for your CA Process Automation data stores with this initial installation.

Consider establishing a naming convention for the databases that contain your CA Process Automation data stores with this initial installation.

Consider housing each data store in its own database for improved performance.

- If you configured the Type of Database as SQL Server or MySQL, the installer will create a database that is named using the value specified in this field.
- If you configured the Type of Database as Oracle, provide an Instance Name or SID. Note that this differs from an Oracle Service Name.

  Note: If you have an Oracle RAC Database or otherwise need to refer to a Service Name, you can configure that as a post-installation task. See Change the Database Configuration to Use an Oracle Service Name (see page 148).

Driver Jar

Defines the JDBC driver JAR file for the specified database type. The drivers folder in the DVD1 folder of the installation media provides default drivers for Microsoft SQL Server and Oracle database servers.

Defaults:

SQL Server: jtds-1.3.jar

Oracle: ojdbc14.jar

MySQL: Click Browse, then navigate to the JAR file you downloaded (for example, mysql-connector-java-5.1.18-bin.jar).

Database Collation

Defines the rules for sorting data for MS SQL and Oracle. Case-sensitivity, accent marks, kana character types, and character width can be part of the rule set. This field is a drop-down list. It is best practice to accept the default value. This field is not applicable to MySQL.

Default: SQL_Latin1_General_CP1_CI_AS

Use Connection String

Select this check box to provide connection string to connect to the Oracle database.

Note: This check box is enabled for Oracle database only.

Connection String

Enter a jdbc connection string in one of the following formats:

`jdbc:oracle:thin:`*`DatabaseServer`*`:`*`PortNumber`*`:`*`DatabaseName`*

`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=`*`hostname`*`)(PORT=`*`portnumber`*`))(CONNECT_DATA=(SERVICE_NAME=`*`serviceid`*`)))`

21. Click Test Database Settings to test connectivity from CA Process Automation to the specified database instance using the specified database port and JAR file.

    If a message indicates that databases are missing, close the message and click Create Database. Except for Oracle, databases that the Orchestrator requires can be created during installation.

    Create Database

    Create the Repository (Library) data store if you specified MS SQL or MySQL.

    Note: When using an Oracle database, you already created the Repository (Library) schema as part of the Oracle database prerequisites.

    A message indicates that a database has been created with the name you provided. Click OK. Click Test Database again.

22. Click Next.

23. 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.

    The Runtime Database fields are similar to the Database Setting fields for the Repository (Library) Database except for two fields. See Step 20 for descriptions of other fields.

    copy from main repository

    Specifies whether to copy the Repository database (also known as Library data store) settings to the Runtime Database settings screen.

    Selected: Copies the Repository database (Library data store) settings to this dialog. This option can save you time if you are using the same database for both CA Process Automation data stores. If you select this option, type the Runtime data store name in the Runtime Database field. Then click Test Database Settings to test connectivity from the Domain Orchestrator to the database server port for the specified database instance. Then click Create Database to invoke the creation of the database for the Runtime data store.

    Cleared: Does not copy the Repository (Library) database settings to this dialog. This option is appropriate if you are using a different type of database for run-time data than you are using for library records.

    Runtime Database

    For MS SQL and MySQL, defines the name of the database in which CA Process Automation run-time instances are stored. No two Orchestrators can point to the same Runtime data store. We recommend that this database be different from the one used by the other data stores.

    For Oracle, defines the Instance Name or SID of the database in which CA Process Automation run-time instances are stored. No two Orchestrators can point to the same Runtime data store. We recommend that you use a different schema in this instance than the one used by the other data stores.

    You cannot share a Runtime data store across Orchestrators. (However, all nodes of an Orchestrator cluster share the same Runtime data store.)

24. Click Next.

25. Configure the Reporting data store in one of the following ways:

    - If you are using the *same* database for the Reporting data store that you are using for the Repository (Library) data store:

        a. Select the copy from main repository check box to automatically enter shared data.

        b. Type the name of the database that the Repository (Library) data store is using in the Reporting Database field.

        c. Click Test Database Settings.

    - If you are using a *different* database for the Reporting data store than you are using for the Repository data store (recommended):

        a. Clear the copy from main repository check box, if needed.

        b. Select the database type from the Type of Database drop-down list.

        c. Complete the User Name field based on the database type:

            For MS SQL or MySQL, enter a user name that is authorized to create and access the database on the database server. (For example, type sa for MS SQL; type root for MySQL.)

            For Oracle, enter a schema that is different from the one used by the Repository data store and which is authorized to create and access the reporting-related database objects.

        d. Complete the Reporting Database field based on the database type:

            For MS SQL and MySQL, type a unique name for the reporting database.

            For Oracle, retain the value unless you want to change the database instance.

        e. Click Test Database Settings.

        f. If the Type of Database is MS SQL or MySQL, click Create Database. (Do not click this button if the Reporting database runs on an Oracle database server.)

    See the following field descriptions:

copy from main repository

Specifies whether to copy Repository (Library) data store settings to the Reporting Database settings screen. The Reporting Database fields are similar to the Database Setting fields for the Repository (Library) Database except for two fields. See Step 20 for descriptions of other fields.

Selected: Copies the Repository Database settings to this dialog. This option can save you time if you are using the same database for both CA Process Automation data stores.

Cleared: Does not copy the Repository Database settings to this dialog. This option is appropriate if you are using a separate database for the reporting data store. We recommend that you dedicate a database for the reporting data store.

Reporting Database

Defines the name of the database that houses the reporting data store.

26. Click Next.
27. Select the additional JAR files, typically JDBC drivers that you want to include in the installation.

    By default, the JDBC drivers that are uploaded in the Third-Party Software installation are displayed and are not selected. You can use the Add Files button to add more JAR files.

    Select each JAR file 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. Use the Add Files button to add more drivers.

    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: For more information about adding and managing Orchestrator and agent resources, including JDBC JAR files, see the *Content Administrator Guide*.

    When you are satisfied with your selection of JAR files, click Next.
28. Monitor the installation progress. The installation program copies and signs all CA Process Automation components. Installation can take a few minutes.
29. Click Finish to exit the installation program.

    Installation of the Domain Orchestrator is complete.

    The initial startup of CA Process Automation after an upgrade or installation can take extra time while the product adjusts the database schema. A rough guide is one hour per GB of data; however, this will vary depending on DBMS vendor, machine specs, and volume of data. Start the Orchestrator (see page 150). Verify the correct operation of this initial Orchestrator before proceeding with installing other system components.

Unattended Domain Orchestrator Installation

CA Process Automation provides the option to install the Domain Orchestrator silently, or unattended, by using 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 you use a copy of this file 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.

Consider the following notes about the response file:

- Do not change the variable names as the installation uses the existing variable names.
- Use forward slashes (/) as directory separators to specify folder locations.
- Use the number sign (#) to comment out variables that you do not want to use.
- See the following installation log to review errors:

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

Follow these steps:

1. Insert Disc 1 of the CA Process Automation installation media or browse to the location where you previously copied the installation files from the installation media.
2. Open the DVD1 folder.
3. Open the following file.

   `response.varfile`
4. Provide the appropriate parameter values.

   The varfile includes parameter descriptions. For example, to enable CA EEM to use the NTLM protocol to authenticate CA Process Automation users, use the following setting:

   `enableNTLM=true`

   Required parameters can be found here.
5. Save the varfile to the path that contains the silent installation script file.

   The response file is created.

Required Parameters in the response.varfile

As mentioned previously, an example response file has been provided in the root folder of DVD1. The parameters that are required to perform an unattended installation of CA Process Automation include the following list. Parameters that are not included in this list are optional.

License

thirdPartyLicenseAccepted

licenseAccepted

Install Location

sys.installationDir

Java Location

javaHome

DVD2 Location

domainInstallerDir

Communication Mode

isSecure (true/false)

Database Details

- databaseType
- dbUserName
- databaseServer
- databasePortNumber
- libDb
- driver
- runtimeDbType
- runtimeDbUserName
- runtimeDbServer
- runtimeDbPort
- runtimeDb
- runtimeDriver
- reportingDbType
- reportingDbUserName
- reportingDbServer
- reportingDbPort

- reportingDb
- reportingDriver

CA EEM Details

- registerApplication (defined as true for an upgrade)
- upgradeApplication (defined as true for an upgrade)
- eiamServer
- eiamAppName
- eiamAdminUsrName
- eiamSDKLevel

New Parameters for CA Process Automation Release 4.2:

nodeCommsV2Port

The port used for simplified communications for the Domain Orchestrator.

eiamSDKLevel

The entry for the CA EEM SDK level.

#hasOracleConnectionString

Specifies whether to provide a connection URL. This is only applicable with Oracle.

#dbOracleConnectionString

JDBC Connection URL.

Example:
`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<database host name>) (PORT=<portnumber>)) (CONNECT_DATA=(SERVICE_NAME=<libDb>))).`

Note: The last two entries appear three times; twice for each database. These parameters are only applicable if you select Oracle as your database and you use a connection string.

Run or Edit the Silent Install Script File

After you create the response file, use one of the following options to start the silent installation:

- Run the silent installation script file and pass its parameters through the command prompt. This option is the best practice when you are installing a single Orchestrator.
- Edit the installation script file parameters, then run the script. This option is the best practice when you are installing multiple Orchestrators.

Use the installation script file that is appropriate for your operating environment:

Note: For UNIX, if you invoke the installation script file using a dollar sign ($) in a parameter, prefix dollar sign ($) with backslash (\). For example, if the database password is 'abc$123', prefix backslash (\) as 'abc\$123'.

Windows

Syntax

```
Silent_Install_windows.bat [Parameter1] [Parameter2]
[Parameter3]...
```

Usage:

```
Silent_Install_windows.bat -VcertPassword=a
-VeiamCertPass=eiamadmin -VeiamPassword=eiamadmin
-VdbPassword=sa -VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

UNIX

Syntax

```
Silent_Install_unix.sh [Parameter1] [Parameter2] [Parameter3]...
```

Usage:

```
Silent_Install_unix.sh -VcertPassword=a -VeiamCertPass=eiamadmin
-VeiamPassword=eiamadmin -VdbPassword=sa
-VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

The installation scripts include the following parameters:

-VcertPassword=*value*

Defines the password that controls access to the keys that encrypt passwords.

-VeiamCertPass

Defines the CA EEM certificate password (for example, pamadmin).

-VeiamPassword

Defines the password for the database that is used for automation objects (for example, pamadmin).

Note: VeiamPassword is the Windows domain password.

-VdbPassword

Defines the password for the database that is used for automation (for example, objectsroot).

-VreportingDbPassword

Defines the password for the reporting database (for example, root).

-VruntimeDbPassword

Defines the password for the database that is used at run time (for example, root).

-VeiamAdminPass

Defines the password for the CA EEM administrator, where the username value is EiamAdmin (for example, eiamadmin).

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

When the installation completes, you can start the Orchestrator. Review the installation.log for any errors after the script executes (install_dir\server\c2o).

Upgrade Considerations (Silent installation)

Before you perform an unattended upgrade to CA Process Automation Release 4.2, locate the response.varfile from your current installation of CA Process Automation.

This file can be found here:

```
<install_dir>\server\c2o\.install4j\response.varfile
```

You need the values for the required parameters (see page 132) to complete the upgrade to CA Process Automation Release 4.2. Once you have obtained those values, start the unattended upgrade with the same command as in a new installation (see page 133).

Note: jTDS drivers are mandatory in CA Process Automation Release 4.2. jtds-1.3.1.jar is included in the drivers folder of DVD1. Any response.varfile parameter from a previous installation that includes a reference to an SQL JAR file must now be replaced with a jTDS value in the CA Process Automation Release 4.2 response.varfile.

For example, a CA Process Automation Release 3.1 response.varfile could include the following parameter:

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drivers/sqljdbc.jar
```

In CA Process Automation Release 4.2, that parameter becomes:

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drivers/jtds-1.3.1.jar
```

Test Your Processes with Simplified Communication

After you have configured agents to use simplified communication, test your processes again.

Follow these steps:

1. Start a process with operators that run on agent touchpoints or on remote hosts through proxy touchpoints. Verify that the process instance completes successfully.
2. When you are satisfied that agents are working as expected with simplified communications, resume all of your normal processing.

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 Enable Secure Communications for Existing CA Process Automation (see page 181).
- If you installed CA Process Automation for the first time:
  - Verify the Port Planning Prerequisites (see page 108) to configure ports.
  - Configure firewalls for bi-directional communication (see page 142).
- To use Databases operators to connect to databases using a different RDBMS than CA Process Automation uses, install drivers for Database operators (see page 143).

  To use Windows Authentication (integrated security) with JDBC for MSSQL Server, install drivers for Database operators (see page 143).
- If you installed the Domain Orchestrator on a server with the HP-UX operating system, perform additional configuration steps on HP-UX.
- If you installed CA EEM with Microsoft Active Directory as the external directory, CA EEM can authenticate users using the NTLM protocol. If you did not elect to enable NTLM pass-through authentication during installation, you can enable it manually now. See Enable NTLM Pass-Through Authentication After Installation (see page 144).
- Tasks such as deploying drivers for Database operators require that you restart the Domain Orchestrator.
  - See Stop the Orchestrator (see page 151).
  - See Start the Orchestrator (see page 150).
- 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 137).

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 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 more information about creating your own user account, see the *Content Administrator Guide*.

To be available, CA Process Automation requires that the following conditions are met:

- CA EEM is running.
- The load balancer, if used, is running.
- The Domain Orchestrator service is started. For more information, see Start the Orchestrator (see page 150).

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

Important! Default administrator credentials are not available if CA EEM is configured to use Microsoft Active Directory as a user store. Default credentials for each user role are available only if you configured CA EEM to use the local user store for creating and storing user accounts.

Follow these steps:

1. Access the appropriate CA Process Automation URL. In the following examples, *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.

   Note: If NTLM Authentication is enabled and your Domain credentials match credentials in an CA EEM user account, the Home tab displays. To support NTLM authentication in Mozilla Firefox, you configure browser settings. For more information, see Mozilla support.

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

   CA Process Automation opens. The Home tab is displayed.

5. From the Help drop-down list, click Book Shelf. Verify the bookshelf can be opened from CA Technologies Customer Support.
6. If needed, make the bookshelf available on Orchestrators without Internet access (see page 139).

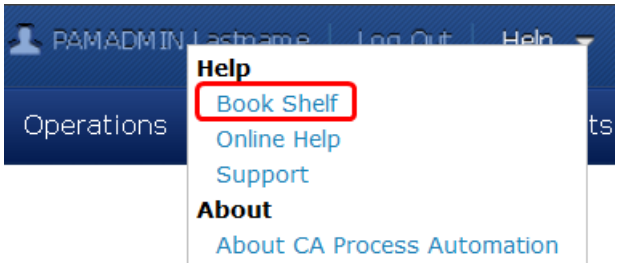
Make the Bookshelf Available on Orchestrators without Internet Access

Users who browse to Orchestrators with Internet access can open CA Process Automation Bookshelf of documentation from the Book Shelf link in CA Process Automation. This link accesses the CA Process Automation Release 4.2 Bookshelf posted on CA Technologies Customer Support (in the language set in User Settings).

Users who browse to Orchestrators that have no Internet access need your help to make the CA Process Automation bookshelf available to them. Activate the Book Shelf link by downloading the bookshelf and moving it to a location that will pick up the local server copy.

Follow these steps:

1. Browse to CA Process Automation and log in as a default administrator (see page 137).
2. From the Help drop-down list, click Book Shelf. Determine whether the bookshelf can be opened from CA Technologies Customer Support.



3. If the bookshelf does not open because Internet access is not provided in the environment where Orchestrators are installed, then perform the following steps.

4. For each language version that CA Process Automation users require, download the bookshelf.zip for that language.
   a. Log on to a computer with Internet access.
   b. Browse to https://support.ca.com
   c. Select Product Documentation from the Get Support tab.
   d. Enter CA Process Automation in the Select a Bookshelf field to get to the relevant part of the drop-down list.
   e. Select a required language.
      - CA Process Automation 04.2.00 -Brazilian Portuguese
      - CA Process Automation 04.2.00 -French
      - CA Process Automation 04.2.00 -German
      - CA Process Automation 04.2.00 -Italian
      - CA Process Automation 04.2.00 -Japanese
      - CA Process Automation 04.2.00 -Spanish
      - CA Process Automation 04.2.00 -Turkish
      - CA Process Automation 04.2.00 -US English
   f. Click Go.

      The selected bookshelf opens.
   g. Click the Download this Bookshelf link. (This link appears above the Release Information section.)
   h. Save the selected bookshelf to your local drive.
   i. Repeat this step, if needed.

5. On each standalone Orchestrator and on each node of each clustered Orchestrator, do the following:

   a. Navigate to the following location:

      install_dir/server/c2o/.c2orepository

   b. Create a folder, bookshelf. That is:

      install_dir/server/c2o/.c2orepository/bookshelf

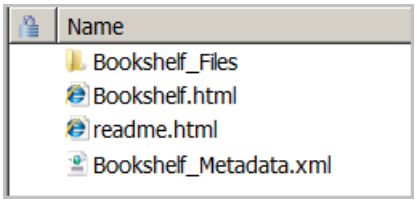
   c. Create a language-specific folder **xx_XX** for each language required by your users. Following is the list of supported languages:

      - de_DE (German)
      - en_US (English)
      - es_ES (Spanish)
      - fr_FR (French)
      - it_IT (Italian)
      - ja_JP (Japanese)
      - pt_BR (Portuguese)
      - tr_TR (Turkish)
      - zh_CN (Chinese)

      For example, the following example directory is for the English translation:

      install_dir/server/c2o/.c2orepository/bookshelf/en_US

   d. Extract the contents of each bookshelf.zip you downloaded to the associated xx_XX language-specific folder.



For example, extract contents for CA Process Automation 04.2.00-ENU.zip to the following directory:

install_dir/server/c2o/.c2orepository/bookshelf/en_US

e. Open CA Process Automation. For example, open CA Process Automation from the Start menu.

f. From the Help drop-down list, click Book Shelf and verify that the bookshelf opens in the default language.

g. If your downloaded the bookshelf.zip in multiple languages, change the language and repeat the previous step to verify that the bookshelf opens in each required language.

To change the language in CA Process Automation, click the User ID link (top, right), which opens User Settings. Set the Language setting.

Configure Firewalls for Bi-directional Communication

CA Process Automation components can be accessed through Web clients. See Ports Used by CA Process Automation (see page 235) for details on the ports used by each component in a CA Process Automation system.

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 with the database that hosts the Library data store.
- The Domain Orchestrator and the database server with the database that hosts the reporting data store.
- The Domain Orchestrator and the database server with the database that hosts the Runtime data store.
- The Domain Orchestrator and CA EEM.
- Each Orchestrator and the database server with the database that hosts the Library data store.
- Each Orchestrator and the database server with the database that hosts the reporting data store.
- Each Orchestrator and the database server with the database that hosts the Runtime data store.

If you use local firewalls on Orchestrator or agent hosts, 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 in the Manage User Resources chapter of the *Content Administrator Guide* for procedures.

Enable NTLM Pass-Through Authentication After Installation

NTLM pass-through authentication enables CA EEM to authenticate users using the NTLM protocol. This is an alternative to using credentials that users enter on the form-based login dialog. With the NTLM pass-through authentication, the login dialog is bypassed.

The following procedure does *not* apply if you already enabled NTLM pass-through authentication, for example:

- You selected the Enable NTLM Pass-Through Authentication during interactive installation of CA Process Automation.
- You specified enableNTLM=true in the response.varfile used for installing CA Process Automation silently.

You can enable NTLM pass-through authentication by manually adding ntlm.enabled=true to the OasisConfig.properties file. Use the following procedure only when you want to enable this feature but did not do it at installation.

Follow these steps:

1. Log in as an administrator to the server where the Domain Orchestrator is installed.
2. Navigate to the following folder, where install_dir refers to the path where the Domain Orchestrator is installed:

   `install_dir/server/c2o/.config`
3. Open the OasisConfig.properties file with an editor.
4. Use Find to locate the following property: ntlm.enabled=
5. Change the value for the property to true, that is:

   `ntlm.enabled=true`
6. Save the file and exit.
7. Restart the Orchestrator service.
   a. Stop the Orchestrator (see page 151).
   b. Start the Orchestrator (see page 150).
8. Repeat this process for each Orchestrator.

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.

Configure CA EEM to Permit Referenced Users to Log in with their Email Name

When you install CA Process Automation, you can configure Global Users/Global Groups in the EEM Server Configuration as Reference from an external directory. You can then select Multiple Active Directory Domains and specify the Microsoft Active Directories (ADs) in which potential CA Process Automation users are defined. During a CA Process Automation installation, you identify the default AD domain. Users belonging the default AD domain can log in to CA Process Automation with their user name and password. Users belonging to other AD domains must enter their principal name and password at login. The standard form for a principal name is *domain**username*.

You can configure CA EEM to authenticate the Active Directory users with their email address, that is, *username@domain*. You configure CA EEM to search for the user using userPrincipalName.

Follow these steps:

1. Log in to CA EEM as the CA EEM administrator and select the application name you set up during the CA Process Automation installation.
2. Select the Configure tab.
3. In the User Store palette, select LDAP Attribute Mapping.

4. Create an attribute map from the existing attribute map by changing the user authentication filter. That is, change samaccountName to userPrincipalName.
   a. Select Microsoft Active Directory from the Mapping Name drop-down list.
   b. In the User Lookup panel, the User Search Filter is similar to the following example:

      ```
      (&(objectClass=user)(!(objectClass=computer)))
      ```

   c. Edit the User Authentication Filter field such that userPrincipalName replaces samaccountName. See the following example results:

      ```
      (&(ObjectClass=user)(!(objectClass=computer)(userPrincipalName= ...
      ```

   d. {UserName} is set as follows:

      ```
      ))
      ```

5. Save the attribute map. For example, type the name **madAuthMail** in the Mapping Name field and then click Save.
6. The User Attribute Mapping data resembles the following data:

   User Name: sAMAccountName

   First Name: givenName

   Last Name: sn

   Display Name: displayName

7. In the General section of the LDAP Directory Configuration, type the attribute map name you created in Step 5. Verify that your entries resemble the following text:

   Name: *domain*

   Attribute Map: madAuthMail

   Domain: *domain*

   Selected Hostnames: *hostname:*389

   Protocol: LDAP

   Base DN: ou=*mylocation*,dc=*mycompany*,dc=com

   User DN: cn=*userid*,ou=Users,ou=*mylocation*,dc=*mycompany*,dc=com

   User Password: *passwordForUserid*

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. All cluster nodes for any Orchestrator must have the same clock time, ideally synchronized with a standard external time server. The load balancer does not handle the time synchronization.

More information:

Synchronize Time for a Cluster Node (see page 207)

How to Install Patches and Connectors with CA Process Automation 4.2

This section describes how to install CA Process Automation Connectors with JBoss 5.1 on a host.

Administrators can install the CA Process Automation Connectors to enable CA Process Automation to interact with other products (CA Products and Third-party Products) to automate business use cases. Each connector acts as a module which contains a set of operators. The operators interact with APIs of other products and are used to create CA Process Automation flows.

As a prerequisite, ensure that you have installed CA Process Automation on the host. The CA Process Automation Connector executable is present on the host.

Important! To successfully install CA Process Automation patch and connector, shutdown all the orchestrator nodes and install the CA Process Automation patch and connector on all nodes (Domain and Non-Domain).

Follow these steps:

1. Run the CA Process Automation Connector Executable.

   The "Welcome to the ..." page appears.

2. Accept the license agreement and click Next.

3. In the Select CA Process Automation Installation Directory page, provide the *install_dir* location.

4. In the Choose Connectors to Install/Update page, select the connectors to be installed and Click Next.

   The CA Process Automation Connector is installed.

5. To verify the CA Process Automation Connector installation, browse to CA Process Automation and log in. Click the Designer tab and click New Process.

   The installed CA Process Automation connector with its operators is listed in the Operators view.

Change the Database Configuration to Use an Oracle Service Name

When you install an Orchestrator using Oracle as the database type, you specify an Oracle Instance Name or SID for each of the three data stores. The Oracle Service Name is required when you reference an Oracle RAC Database; you configure CA Process Automation to use an Oracle Service Name as a post-installation task.

In the examples that follow, replace the *oracle-hostname-or-ip* variable with one of the following values:

- The host name of an Oracle RAC SCAN
- The IP address of an Oracle RAC SCAN
- The host name of a standalone Oracle instance
- The IP address of a standalone Oracle instance

Follow these steps:

1. Verify that CA Process Automation successfully uses the Oracle databases that were specified (at installation) using the Instance Name or SID. To verify successful usage, start the CA Process Automation service and examine the log file to verify that there are no database-related errors. The log file path and name is:

   `install_dir/server/c20/logs/c2o.log`

2. Stop the CA Process Automation service as described in Stop the Orchestrator (see page 151).

3. Open the OasisConfig.properties file.

   `install_dir``\server\c2o\.config\OasisConfig.properties`

4. Modify the following entries for the Library data store:

   ```
   oasis.database.connectionurl=jdbc:oracle:thin:@//oracle-hostname-or-ip:1521/
   oasis.database.lib.dbname=ServiceName
   oasis.database.queues.dbname=ServiceName
   oasis.database.dbhostname=oracle-hostname-or-ip
   ```

5. Modify the following entries for the Runtime data store:

   ```
   oasis.runtime.database.connectionurl=jdbc:oracle:thin:@//oracle-hostname-or-ip:1521/
   oasis.runtime.database.dbname=ServiceName
   oasis.runtime.database.dbhostname=oracle-hostname-or-ip
   ```

6. Modify the following entries for the Reporting data store:

   ```
   oasis.reporting.database.connectionurl=jdbc:oracle:thin:@//oracle-hostname-or-ip:1521/
   oasis.reporting.database.dbname=ServiceName
   oasis.reporting.database.dbhostname=oracle-hostname-or-ip
   ```

7. Save the OasisConfig.properties file.

8. Start the Orchestrator (see page 150).

For the connection URL statements, the following notations are also valid:

Referencing an Oracle Hostname using TNS Notation

The following example is not RAC-specific.

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=Oracle-hostname-or-ip)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ServiceName)))
```

Referencing RAC Virtual Host Names using an Address List with TNS Notation

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=OFF)(FAILOVER=ON)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-hostname-or-ip)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-hostname-or-ip)(PORT=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=ServiceName)))
```

Important! When using TNS notation, ensure that the .dbname value for each of the data stores is blank, The .dbname value is appended onto the connection URL statement when connecting to the database. Appending the service name is not desired in this case, as it is included in the TNS notation.

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 the 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. Perform one of the following tasks:
   - Select Programs, CA, CA Process Automation, 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:

     `install_dir``/server/c2o/bin/startc2osvc.bat`
3. If you logged in to a UNIX or Linux host, perform the following tasks:
   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.

Stop the Orchestrator

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

Important! If an Orchestrator is not shut down gracefully, the following temporary folder can build up several gigabytes of files. If this happens, you can safely delete the tmp folder:

install_dir/server/c2o/tmp

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. Complete one of the following actions:
   - 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:

     install_dir/server/c2o/bin/stopc2osvc.bat
3. If you logged in to a UNIX or Linux host, complete the following steps:
   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. For example:

      ./c2osvrd.sh stop

Uninstall the Domain Orchestrator

Only administrators with administrator credentials on the server where the Domain Orchestrator is installed can uninstall it.

Note: Stop the Domain Orchestrator before uninstalling it.

Follow these steps:

1. Using the Administrator credentials, log in to host where the target Domain Orchestrator is installed.
2. If you logged in to the following hosts:
   a. A Windows host:
   You can uninstall the Domain Orchestrator from the Start menu and Control Panel. Perform one the following tasks:
      - Select Programs, CA, CA Process Automation 4.2, and Uninstall CA Process Automation from the Start menu.
      - Select the CA Process Automation Domain entry from the Start menu, Control Panel, Programs and Features, and click Uninstall.

        The Uninstall wizard is displayed.

   b. A UNIX or Linux host, perform the following tasks:
      a. Change directories to ${PAM_HOME}/standalone/. For example, change directories to:

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

      b. Run the ./uninstall script.

         The Uninstall wizard is displayed.
3. After the Domain Orchestrator is uninstalled, verify the following changes:
   - In Administrative Tools and Services from the Control Panel, the CA Process Automation Domain service is deleted.
   - The CA Process Automation Domain entry is removed from the Start menu, Control Panel, Programs and Features.
   - The Domain Orchestrator folder is removed from the Installation location.

Chapter 6: Upgrade to the Current Release

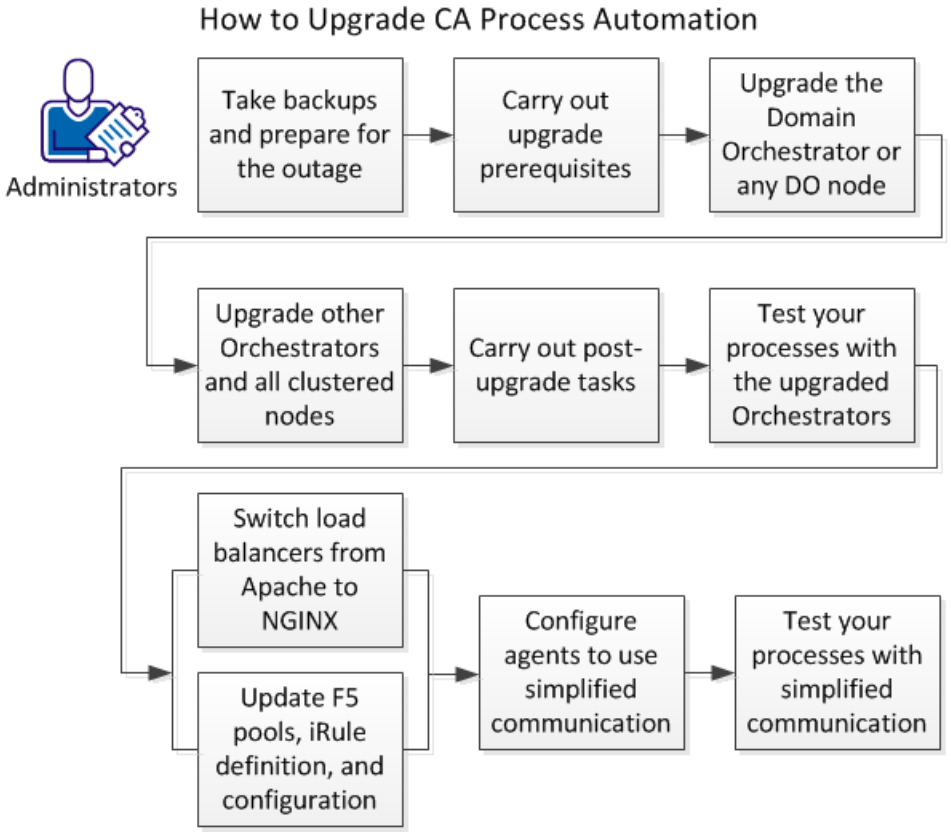
You can upgrade to CA Process Automation Release 4.2 from the following CA Process Automation releases:

- CA Process Automation Service Pack 03.1.01 (3.1 SP01)
- CA Process Automation Service Pack 04.0.01 (4.0 SP01)
- CA Process Automation Release 04.1.00 (4.1)
- CA Process Automation Service Pack 04.1.01 (4.1 SP01)

This section contains the following topics:

How to Upgrade CA Process Automation

You can upgrade to CA Process Automation Release 4.2 from Release 3.1 SP01 and above using the illustrated process.



Important!

- If needed, upgrade from a release prior to r3.1 SP01 (see page 284) before you begin the process that is documented here.
- If the Orchestrators you are upgrading are installed on 32-bit hosts, see TEC596124 for guidance on migrating to 64-bit hosts.
- Before you upgrade CA Process Automation, the value calculation of the *Minimum Number of Finished (Completed, Failed, Aborted) Instances* field includes the Failed Instances. After you upgrade CA Process Automation, the Field label changes to *Minimum Number of Finished (Completed, Aborted) Instances* and the value calculation does not include the Failed Instances.

Follow these steps:

1. Take backups and prepare for the outage (see page 155).
2. Carry out upgrade prerequisites (see page 156).
3. Upgrade the Domain Orchestrator (see page 158).
4. Upgrade other Orchestrators and all clustered nodes.
   - Upgrade a Nonclustered Orchestrator (see page 162).
   - Upgrade a Cluster Node (see page 164).
5. Carry out post-upgrade tasks (see page 167).
6. Test your processes with the upgraded Orchestrators (see page 168).
7. One of the following:
   - Switch load balancers from Apache to NGINX (see page 169).
   - Update F5 Pools, iRule definition, and configuration (see page 169).
8. Configure agents to use simplified communication (see page 170).
9. Test your processes with simplified communications (see page 136).

Take Backups and Prepare for the Outage

Unforeseen or uncontrollable incidents may interrupt or otherwise cause the upgrade process to fail. As a precaution, we recommend that you back up all valuable data stored in CA Process Automation folders before you begin the upgrade. To prepare for full rollback, also back up:

- The databases that contain the CA Process Automation data stores.
- The CA Process Automation authentication and authorization policies stored in CA EEM.

Follow these steps:

1. Verify that your databases have access to at least double the space that is currently used by your existing CA Process Automation data stores.
2. To prepare for potential rollback, either snapshot all Orchestrator VMs or back up the following folder on all Orchestrators:

   install_dir/

   The best practice is to back up this folder to a different physical disk than the one that hosts the *install_dir* folder. The JBoss files are in the install_dir folder. The ability to restore the previous version depends on this folder being backed up.

   To back up hotfixes or connector installation, copy only the *install_dir*/server/c2o/ folder.

3. Back up the library, runtime, and reporting data stores used by each Orchestrator before you upgrade. Data stores can reside in separate databases or all in the same database.
4. Back up the CA Process Automation application in your CA EEM server.
   a. Log into CA EEM, specifying the CA Process Automation application.
   b. Click the Configure tab, click EEM Server, and click Export application.
   c. Click Export and save the <application-name>.xml.gz file to your local drive.
5. Prepare for an outage. The duration of an Orchestrator upgrade depends on the size of the data stores. The more data you have, the longer the upgrade takes.
   - If you have other applications that rely on CA Process Automation services, prepare for this outage. For example, if you use Service Catalog to initiate CA Process Automation processes, you could shut down Service Catalog during the CA Process Automation upgrade. Alternatively, you could present a "temporarily unavailable" dialog for catalog items that rely on CA Process Automation and then remove that dialog when the CA Process Automation upgrade completes.
   - Schedule an appropriate maintenance window and inform relevant stakeholders about the interval when you expect CA Process Automation to be unavailable.

Carry Out Upgrade Prerequisites

Before you start the process to upgrade to CA Process Automation Release 04.2.00, complete the following prerequisite tasks:

1. Have at hand the CA EEM administrator credentials, where EiamAdmin is typically the EEM Admin Username, and the EEM Admin Password is known to the CA EEM administrator.
2. Record the Certificate Password to use for this system upgrade.

   The certificate password is used to control access to the keys used to encrypt passwords and other critical data. You specify this password for the first Orchestrator you upgrade. Then, you must enter this same password when you install other nodes of the Domain Orchestrator, other standalone Orchestrators, and nodes of other clustered Orchestrators for the same release.
3. Ensure that no CA Process Automation processes are currently active, that is, in a Running state or Blocked state.
4. Shut down all non-domain Orchestrators. For clustered non-domain Orchestrators, shut down the Orchestrator service on each node. See Stop the Orchestrator (see page 151).

5. Shut down the Domain Orchestrator. For a clustered Domain Orchestrator, shut down the Orchestrator service on each node. See Stop the Orchestrator (see page 151).

   Notes:

   - Active agents are unable to connect to Orchestrators that are shut down, but will reconnect when the Orchestrators are restarted.
   - Scheduled processes and operators will not run during the upgrade process.

6. If you use an Apache load balancer, copy the updated Apache configuration templates from DVD1. For details, see Apache Load Balancer (see page 32).

7. If you use an F5 load balancer, update the iRule definition to remove the Primary Node designation. This change makes it possible to continue to use the deprecated communication for the first phase of the upgrade.

   a. Remove: set PRIMARY "[PrimaryIP]"

   b. Remove: set PRIMPORT "[PrimaryPort]"

   c. Remove all occurrences: member $PRIMARY $PRIMPORT

8. Verify that the version of the JDK installed on all Orchestrator nodes is a supported version. See JDK Prerequisites (see page 93).

9. If the DNS host name defined when you installed CA Process Automation contained restricted characters (such as underscores), correct the DNS host name. For more information, see Resolve Invalid Character in CA Process Automation DNS Name (see page 252).

10. Verify that CA EEM is running and that it is a release that CA Process Automation supports. CA EEM is the required directory server.

    Note: CA Process Automation Release 4.2 supports CA EEM Releases 8.4 SP04 CR10 through 12.51.

    a. If you have no available CA EEM instance, download installers for CA EEM 12.51 from the same location as the CA Process Automation installation media. Follow the instructions provided in the CA EEM documentation when deploying your CA EEM instance. The ISO on download location on support.ca.com contains server downloads for all platforms for CA EEM Release 12.51 and the related documentation zip file.

    b. If you are using a release prior to 12.51, consider upgrading if you want to take advantage of these new features:

       - Support of 2048- and 4096-bit security certificates requires CA EEM Release 12.5 or later (English) and Release 12.51 (other supported languages).
       - Support of multiple Microsoft Active Directory Domains requires CA EEM version 12.0 or later. This option is available when you configure CA EEM to reference an external user store.

         Note: CA EEM Release 8.4 SP04 CR10 supports referencing a single LDAP directory.

       Follow the instructions provided in the CA EEM documentation when upgrading your CA EEM instance.

Upgrade the Domain Orchestrator

You can upgrade directly to CA Process Automation Release 4.2 from the following CA Process Automation versions:

- CA Process Automation Service Pack 3.1 SP01
- CA Process Automation Service Pack 4.0 SP01
- CA Process Automation Release 4.1
- CA Process Automation Service Pack 4.1 SP01

If the Domain Orchestrator is clustered, you can begin the upgrade with any node, using the following procedure. When you upgrade subsequent nodes, the process is similar to Upgrade a Cluster Node (see page 164), which is written for non-Domain clustered Orchestrators. The main difference is that you invoke the upgrade by selecting the Install Cluster Node For Domain Orchestrator option on the Installation palette.

Follow these steps:

1. Log in to the host on which the Domain Orchestrator (or a Domain Orchestrator cluster node) is installed.
2. Navigate to the DVD1 folder on the installation media and start the installation wizard from the file for your operating system. These files invoke the third-party installer and then the Domain Orchestrator installer.
   - **Windows:** Domain_Installer_windows.bat
   - **Linux or UNIX:** Domain_Installer_unix.sh

     Note: The Domain_Installer_unix.sh is *not* a command line script. You must invoke it with a display for the GUI installation.
3. Click Next to move through the initial pages of the wizard:
   - Language
   - Welcome to the CA Process Automation 3rd Party Installer Setup Wizard
   - License agreement - I accept the terms of the License Agreement
4. On the Select Destination Directory page, navigate to the *same* directory that you used for the previous release. (If you specify a different directory, this installation is treated as a new Orchestrator rather than an upgraded Orchestrator.)

   In Windows, the following are default paths up to the original installation folder:

   Release 3.1 SP01

   ```
   C:\program files\ca\itpam
   ```

   Release 4.0 and above

   ```
   C:\program files\ca\pam
   ```
5. If the Reinstall page appears, select Reinstall to proceed with the upgrade.
6. Click Next to Prerequisites for CA Process Automation Installation.

7. When the JDBC Jars Installation appears, click Add Files to install the required drivers.

   - 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 JTDS JDBC jar file on DVD1 installation disk. For example:

     `...\DVD1\drivers\jtds-1.3.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.

8. When the Completing the CA Process Automation Setup Wizard appears, replace DVD1 with DVD2 in the Directory path. Then click Finish.

   The message appears: "Copying CA Process Automation installer. This may take a few minutes to complete, please wait." You may experience a time lag between the close of this page and the opening of the Welcome page.

9. When the Welcome to CA Process Automation Domain Setup Wizard appears, click through the initial pages of the wizard:

   - Welcome to the CA Process Automation Domain Setup Wizard
   - License Agreement- I accept the terms of the License Agreement

10. Verify that the Java Home Directory points to the version of JDK that this release supports.

11. Continue, clicking through pages:

    - Reinstall
    - Configuration Screen

12. When the Set Certificate Password appears, enter the password that was specified during the installation of the last release. You must specify this same password to upgrade all other Orchestrators, Orchestrator nodes, and agents in this CA Process Automation Domain. Click Next.

13. Click through the Select Start Menu Folder to use your previous selection.
14. On the General Properties page, note the following changes in defaults for the Orchestrator server port:

    Server Port

    Defines the port that the Domain Orchestrator uses to communicate with other Orchestrators and agents. This port is used by simplified communication.

    Default: 80 (basic: HTTP), or 443 (secured: HTTPS)

    Deprecated Server Port

    The Server Port value that was defined for a previous release of CA Process Automation. This port is used by deprecated communication.

    Default: 7001
15. Click through the following pages, making changes at your discretion.
    - Scripts Temporary Directory
    - Powershell Execution Policy
16. When the Embedded Entitlements Manager (EEM) Security Settings appears,
    a. Verify that the application name listed is the correct EEM application name for the CA Process Automation instance that you are upgrading.

       This name can be customized, so the correct application name may not be shown by default.
    b. Select Register Application with CA EEM and click Register.
    c. Supply credentials for logging into CA EEM as the EiamAdmin administrator.
    d. Agree to upgrade. The installation process detects the CA EEM server version and chooses the appropriate SDK.
    e. Click OK when the Application Registered confirmation appears.
17. Click through the Database Settings since you have already defined these:
    - Repository database
    - Runtime database
    - Reporting database
18. Click through Additional JARs for installation if there is nothing to add.

19. When the Completing the CA Process Automation Domain Setup Wizard appears, click Finish.

    Important! It takes a significant amount of time before the Domain Orchestrator becomes available for login. The upgrade of additional Orchestrators or additional nodes, if the Domain Orchestrator is clustered, can begin only after you can log on to the Domain Orchestrator.

20. Start the Orchestrator service on the Domain Orchestrator.

    Note: See Start Orchestrators (see page 150) for operating system-specific details.

21. Continue in one of the following:

    - If you have other Orchestrator or cluster nodes:

      Upgrade a Nonclustered Orchestrator (see page 162)

      Upgrade a Cluster Node (see page 164)

    - If your only Orchestrator is a Nonclustered Domain Orchestrator:

      Carry out post-upgrade tasks (see page 167)

More information:

Upgrade Considerations (Silent installation) (see page 135)

Upgrade a Nonclustered Orchestrator

After you upgrade the Domain Orchestrator by invoking a script distributed on the media, you can upgrade other Orchestrators from the CA Process Automation UI.

Follow these steps:

1. Log in to the host on with the Orchestrator to upgrade.
2. Browse to CA Process Automation and log in (see page 186) with administrator credentials.
3. Click the Configuration tab and select the Installation palette.
4. Click Install in the Install Orchestrator section to begin the upgrade.
5. Select a language and click OK.

   The Welcome to the CA Process Automation Third-Party Installer Setup wizard page appears.

6. On the Licensing agreement page, select the option to accept the agreement, and then click Next.
7. On the Select Destination Directory page, navigate to the directory that you used for the previous release. For example, in Windows, the following are defaults, depending on the source release.

   `C:\program files\ca\itpam`

   `C:\program files\ca\pam`
8. Click Next to Prerequisites for CA Process Automation Installation.
9. Specify JDBC jars for installation in one of the following ways:
   - To use the same JDBC jars as the Domain Orchestrator, leave the Use Domain check box selected and click Next.
   - To use different JDBC jars than the Domain Orchestrator uses, clear the Use Domain check box and do the following:
     a. Click Add Files.
     b. Select the database type.
     c. Click Browse and navigate to the JDBC JAR file for the selected server type.
     d. Click Next.
10. Click Next to confirm, and then click Finish to advance to the CA Process Automation installer.
11. Click Next on the Welcome page
12. Select the option to accept the license agreement and click Next.
13. When the Java Home Directory page appears, browse to the location of the upgraded JDK and then click Next.
14. Click Next to proceed through the following installation wizard pages:
    - Domain URL
    - Single Sign-on and Load Balancer configuration page
    - Company Name
15. Enter the certificate password, and click Next.

    Important! This entry must match the certificate password that was entered when the Domain Orchestrator was upgraded.

16. Click Next to accept the previous configuration on following installation wizard pages:
    - Start Menu Folder preferences and click Next.
    - General Properties
    - Scripts temporary directory
    - PowerShell run policy
    - Repository database settings for this Orchestrator
    - Runtime database settings
    - Reporting database settings
17. Click Finish.
18. When processing completes, start the Orchestrator service on the upgraded nonclustered Orchestrator.

    Note: See Start Orchestrators (see page 150) for operating system-specific details.

More Information:

Example: Upgrade a Non-clustered Orchestrator from 4.1 SP01 to Release 4.2 on Windows (see page 279)

Upgrade a Cluster Node

When you upgrade a clustered Orchestrator, you upgrade one node at a time, beginning with any node in the cluster.

Follow these steps:

1. Log onto the host on which a cluster node is installed.
2. Browse to the Domain Orchestrator URL (the load balancer for the Domain Orchestrator, if clustered).
3. Log in, click the Configuration tab, and then click the Installation palette.

4. Under Install Cluster Node for Orchestrator, click Install to begin the upgrade.
5. The language selection dialog appears first. Click OK.
6. Click Next to the Welcome to the CA Process Automation 3rd Party Installer Setup Wizard page.
7. For License Agreement, select I accept the terms of the license Agreement and then click Next.
8. On the Select Destination Directory page, navigate to the directory you used for the previous release. For example, in Windows, the following are defaults, depending on the source release.

   `C:\program files\ca\itpam`

   `C:\program files\ca\pam`
9. Click through the following Wizard pages:
   - Prerequisites for A Process Automation installation - invokes installation.
   - Completing the CA Process Automation Setup Wizard with Use Domain selected - Click Finish

     Wait until the next page appears. There is no visual indicator of the processing that precedes the display of the next page.
   - Welcome to the CA Process Automation Domain Setup Wizard
   - License Agreement
10. If you upgraded your JDK, browse to the Java Home Directory, for example, C:\Program Files\Java\jdk1.7.0_45
11. Complete the Configuration Screen:
    a. If you have already upgraded a node in this cluster, select from the Orchestrator drop-down list the Orchestrator node that you upgraded first.
    b. Type node1, node2, node3, or node4 in the Load Balancer Worker Node field to identify the node you are upgrading.
12. Type your company name, if not displayed
13. Enter the certificate password.

    Important! This entry must match the certificate password that was entered when the Domain Orchestrator was upgraded.

14. Click through the following pages, if they appear. Settings used by node1 are used by other nodes in the cluster.
    - Select Start Menu Folder.
    - General Properties page (Install as Windows Service is not shown but is assumed).
    - Scripts Temporary Directory
    - PowerShell
    - CA Embedded Entitlements Manager (CA EEM) Security Settings
    - Database Settings - Repository
    - Database Settings - Runtime
    - Database Settings - Reporting

    The upgrade installation begins.
15. When Completing the CA Process Automation Setup Wizard page appears, click Finish.

    Processing continues after you click Finish.
16. When processing completes, start the Orchestrator service on the upgraded cluster node.

    Note: See Start Orchestrators (see page 150) for operating system-specific details.

More information:

Example: Upgrade Any Node of the Domain Orchestrator from 3.1 SP01 to Release 4.2 on Windows (see page 271)
Example: Upgrade Another Node of the Domain Orchestrator from 3.1 SP01 to Release 4.2 on Windows (see page 276)

Carry Out Post-Upgrade Tasks

The post-upgrade tasks for agents depends on the following factors:

- Whether you specified the same Certificate Password during Orchestrator upgrades as you specified in the previous release or whether you specified a new Certificate Password. Orchestrators and agents share the same Certificate Password.
- The release from which you are upgrading.

After you upgrade to CA Process Automation Release 4.2, complete the post-upgrade tasks.

Follow these steps:

1. (Optional) Carry forward any of the following configuration file modifications that you want to retain.
   a. Navigate to the following backup location:

      `install_dir/config_backup_MM_dd_yyyy_HHmm`

   b. Use a file comparison tool to highlight differences between the following backed up configuration files and current CA Process Automation version.
      `install_dir/server/c2o/.config/OasisConfig.properties`
      `install_dir/server/c2o/bin/c2osvcw.conf`
      `install_dir/server/c2o/conf/standardjboss.xml`
      `install_dir/server/c2o/conf/log4j.xml`

   c. Apply appropriate changes to the current CA Process Automation version.

      See also Tuning CA Process Automation by Editing Configuration Files (see page 227).

2. Browse to CA Process Automation and log in (see page 186).
3. Click the Configuration tab and examine the Configuration Browser.

4. Verify that all Orchestrators appear under the Orchestrators node and that the associated Orchestrator touchpoints appear in the Domain hierarchy under the correct environment. If any Orchestrator is not active, start the Orchestrator (see page 150).
5. Verify that agents have restarted. Agents using deprecated communication restart automatically. (Start agents (see page 194) that are running but not responding, or are not running.)
6. If your Orchestrators have no Internet access, make the bookshelf available on Orchestrators without Internet access (see page 139).
7. If you are using CA EEM 12.51 with your upgraded CA Process Automation and you configured CA EEM to reference multiple Microsoft Active Directories or an AD forest:
   a. Recreate CA Process Automation users in CA EEM.
   b. Reinstate object ownership.

   Notes:

   - See "Manage Access for Referenced User Accounts" in the *Content Designer Guide*.
   - See "Change Ownership for an Automation Object" in the *Content Designer Guide*.
8. Upgrade any CA Process Automation connectors that are not 4.x connectors.

Test Your Processes with the Upgraded Orchestrators

After the upgrade is complete, test your processes with the upgraded CA Process Automation. Consider the following approach. Verify that processes run successfully on each of your Orchestrators.

Follow these steps:

1. Start a process that generates a task. Take the task for yourself. Verify that the process instance appears on the Home tab. Verify that the task you took appears in your Task List.
2. Start a scheduled process or operator. Verify that it starts on time and completes successfully.
3. Start a process with operators that run on agent touchpoints or on remote hosts through proxy touchpoints. Verify that the process instance completes successfully.
4. Allow solutions that use CA Process Automation as an integrated component to run. Monitor the results and verify that nothing unexpected occurs.

Switch Load Balancers from Apache to NGINX

If you used an Apache load balancer for your clustered Orchestrators prior to upgrade, we recommend that you retain this load balancer until you have verified that everything is working smoothly with your new release. This requires that you update your Apache configuration with new templates provided in the installation media.

The change to NGINX after an upgrade is no different from setting up NGINX in a new release except that for upgrades, you install NGINX on the same server where the Apache load balancer currently exists. This lets you leverage the previously established URL and the previously established host names and ports.

For details on the setup, see NGINX Load Balancer (see page 63).

Agents communicate with Orchestrators; Orchestrators communicate with agents. Release 4.2 introduces an improved simplified communication method. Apache uses the deprecated communication method. By default, existing agents are configured to use deprecated communication. This default setting allows you to switch load balancers from Apache to NGINX and convert existing agents to use simplified communication at a convenient time after you complete the mandatory upgrade tasks. NGINX supports simplified communication. (NGINX also supports deprecated communication.)

Update F5 Pools, iRule Definition, and Configuration

To use simplified communication, modify the F5 configuration.

Follow these steps:

1. Create two F5 pools for each CA Process Automation cluster (see page 54).
2. Replace your current iRule with The iRule Definition (see page 57).
3. Configure F5 to use simplified communication with HTTPS (see page 60).

Configure Agents to Use Simplified Communication

You can configure agents to use simplified communication, for example, in the second phase of the upgrade. There are two approaches:

- Change the communication type from the Configuration tab (described here).
- Reinstall the agents, where the Use Deprecated Communication check box is cleared.

  Agent reinstallation uses the same procedure as a new agent installation.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent for which to switch communication and click Lock.
3. Select the Properties tab for the selected agent.
4. Clear the Use Deprecated Communication check box.
5. Select the agent and click Unlock.
6. Click Yes on the Unsaved Data dialog to save the changes.

   The agent creates web socket connections and sends connection details to all Orchestrator nodes. Orchestrators use the persisted web socket connection to send requests or updates to the agent as needed.
7. Restart the agent (see page 194).
8. Repeat this procedure for each existing agent.

Important! If you later change the Domain Orchestrator communication type from basic communication to secure communication (that is, the HTTP protocol with port 80 to the HTTPS protocol with port 443), you must reinstall the agents (see page 186) that use simplified communications.

About Agent Communication

You configure agent communications when you install an agent. You can reconfigure this setting without reinstalling the agent.

Simplified Communication

The simplified communication uses web sockets and HTTP to produce a one way, persistent connection from the agent to the Orchestrator. CA Process Automation uses a standard port (80 or 443) that provides a fast connection between the components.

Deprecated Communication

The deprecated communication, which uses multiple ports, is not as firewall-friendly or NAT router-friendly as simplified communication. The Orchestrator-initiated connections used in deprecated communication is not as efficient as the persistent connections used in simplified communication.

Note: For recommendations on load balancers and the corresponding agent communication, see "Load Balancers and Communication" in the *Installation Guide*.

More Information

Ports Used by the Load Balancer (see page 238)

Chapter 7: Reinstall or Configure the Current Release

You can make changes to the current Orchestrator release version by rerunning the installation wizard. Options include "Reinstall" and "Configure the Existing Installation."

This section contains the following topics:

Example Scenario: Configure the Existing Installation to Regenerate CA Process Automation Certificates

When you run the installation process for the release you previously installed, you have the option to reinstall or to configure the existing installation. This example scenario shows how to use the configure existing installation option to regenerate certificates that CA Process Automation uses to connect to CA EEM.

The Domain Orchestrator installation process lets you register (or re-register) CA Process Automation with CA EEM. This registration process generates application certificates for CA Process Automation with the same key length as the certificates that CA EEM uses.

Note: CA Process Automation has other certificates that are unaffected by registration; registration only generates the certificates that CA Process Automation uses to connect to CA EEM. The certificate location is *install_dir*/server/c2o/.c2orepository/public/certification.

This example scenario assumes the following setup:

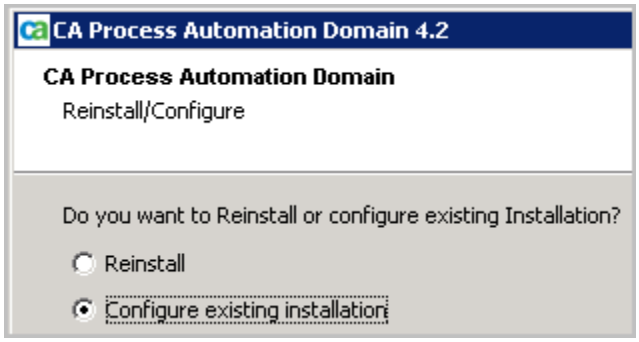
1. The CA EEM administrator installs or upgrades to CA EEM Release 12.51 with default certificates, which have 1024-bit keys.
2. You install or upgrade to CA Process Automation Release 4.2. The generated CA Process Automation certificates also have 1024-bit keys.
3. Later, the CA EEM administrator generates new CA EEM certificates with longer key lengths (2048-bit or 4096-bit).

In this case, use the following procedure to regenerate CA Process Automation certificates with key lengths that match those of the CA EEM certificates.

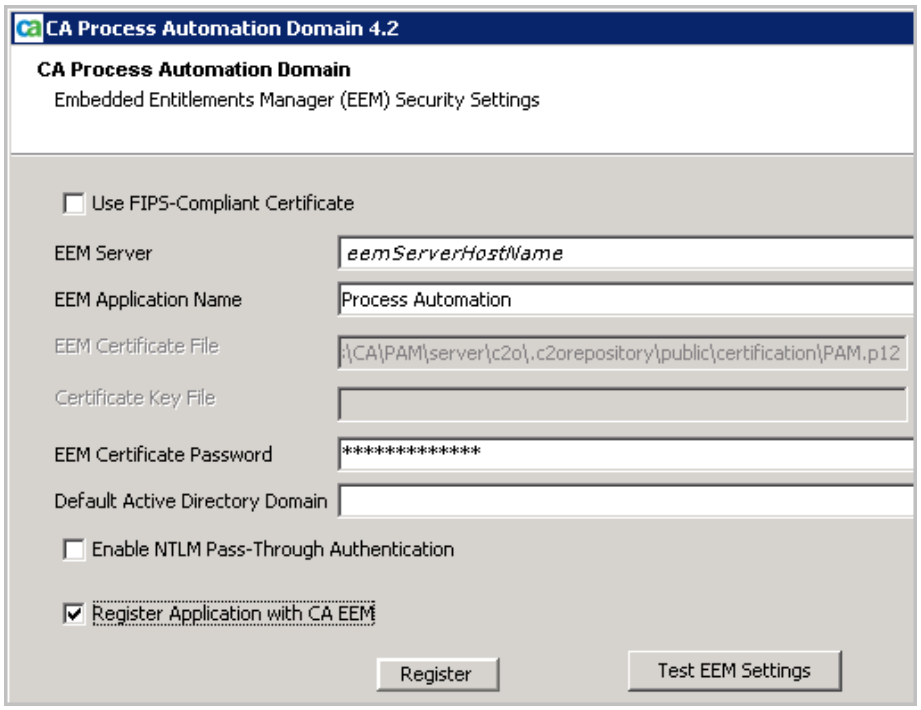
Follow these steps:

1. Install the Third Party Software (see page 109).

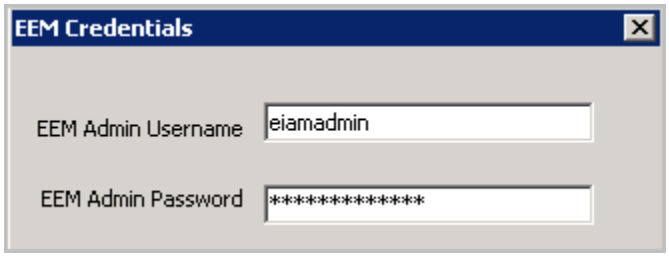
   When the third-party software installation completes, the CA Process Automation Domain Setup installation process starts.
2. Click through the initial pages until the Reinstall/Configure page appears.
3. Select Configure existing installation. (This process modifies the properties files; it does not modify any JARs.)



4. Click through the pages until Embedded Entitlements Manager (EEM) Security Settings page appears.
5. Select the Register Application with CA EEM check box and then click Register.

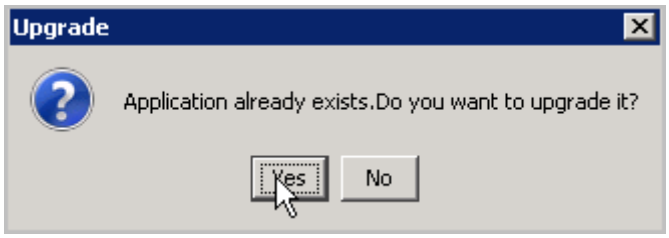


6. Enter the credentials of the CA EEM administrator. Type **EiamAdmin** for the EEM Admin Username. Enter the associated password.



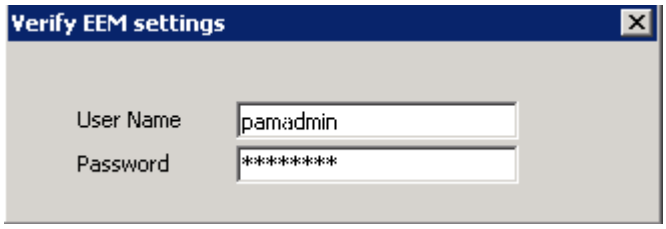
7. Click Yes to upgrade the application even though you are not upgrading the CA Process Automation release.

   (Clicking Yes is required for the generation of the application certificates that CA Process Automation needs.)

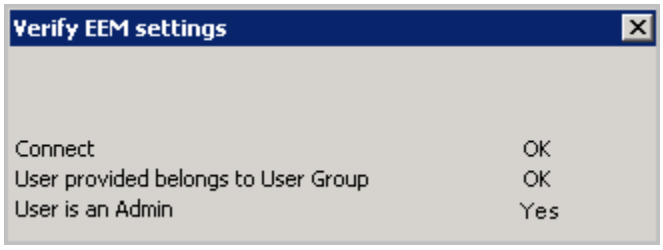


8. Click Test EEM Settings. Click OK to Setup messages.
9. Enter the credentials of a CA Process Automation user who is assigned to the PAMAdmins group.

   Note: The example entry of **pamadmin**, **pamadmin**, is valid only **if** you configured CA EEM to use the internal user store.



10. Verify that CA Process Automation connects to CA EEM and that CA EEM authenticates the credentials.



11. Click through the rest of the installation process and then click Finish.

Post-installation Support for CA EEM Upgrades

If you are running the installation process against the same CA Process Automation version, you are presented with the following options:

Reinstall

Displays the entire installation wizard.

Select Reinstall if your previous installation used the CA EEM Release 8.4 server but you have upgraded the CA EEM server to Release 12.

- If you register the application with CA EEM Release 12.x, the reinstall processing selects the CA EEM major version 12 SDK.
- If you do not register the application, the reinstallation process prompts you to select an SDK based on your version of CA EEM.

Select Reinstall if you use CA EEM Release 12.5 but your SDK version is major version 8. The reinstall process updates the SDK to major version 12.

Note: CA Process Automation can use CA EEM SDK major version 8 with CA EEM Release 12.x. Upgrading the SDK to major version 12 lets you use the new CA EEM features.

Configure the existing installation

Displays only selected pages. (This process modifies the properties files; it does not modify any JARs.)

Select this option if you generated CA EEM certificates with longer key lengths (2048 or 4096) after you installed or upgraded CA Process Automation to Release 4.2.

When you click Register on the CA EEM configuration page, CA Process Automation prompts you to upgrade the existing application in CA EEM. When you agree to upgrade, CA Process Automation certificates (used to communicate with CA EEM) are regenerated. The new CA Process Automation certificates have key lengths matching the lengths of CA EEM certificates.

Note: See the CA EEM documentation for more information about upgrading CA EEM or its certificates.

CA Process Automation uses the CA EEM SDK to communicate with CA EEM; communication is secured with certificates. Both CA EEM and CA Process Automation have certificates. CA Process Automation certificates must have the same key length as CA EEM certificates.

During CA Process Automation Release 4.2 installation or upgrade to Release 4.2, the installation process retrieves the CA Process Automation certificates from CA EEM and chooses the appropriate SDK for the associated CA EEM. These certificates can be found here:

install_dir/server/c2o/.c2orepository/public/certification

As long as CA EEM is not changed, no action is required. However, the following changes to CA EEM require your action.

Install CA Process Automation Release 4.2 with CA EEM Release 8.4 and then upgrade CA EEM to Release 12.x

It is possible to take no action and still use CA Process Automation with CA EEM as long as the CA EEM certificates are generated with the default key lengths. CA Process Automation can use the CA EEM SDK major version 8 to communicate with CA EEM Release 12.x. However, the CA EEM SDK major version 12 allows you to take advantage of new features in CA EEM 12.x.

We recommend that you (1) upgrade the certificates that CA Process Automation uses to communicate with CA EEM and (2) upgrade CA Process Automation to use the CA EEM SDK major version 12. To do this, rerun the installer. The following procedure references step numbers from Install the Domain Orchestrator (see page 111).

- Step 5: Select **Reinstall** (not "Configure the existing installation")
- Step 16: Select the **Register Application with CA EEM** check box.
- Step 17: Click **Register**, select **Yes** to the prompt to upgrade, click **OK** when the Application Registered confirmation appears.

Install CA Process Automation Release 4.2 with CA EEM Release 12.51 and then generate new CA EEM certificates with 2048 or 4096 key lengths

1. CA Process Automation Release 4.2 is installed with CA EEM Release 12.51 using certificates with 1024-bit key lengths.
2. You generate new CA EEM certificates with 2048 (or 4096) key lengths.
3. You re-run the CA Process Automation installation wizard, but this time you select Configure existing installation (not Reinstall).
4. You register CA Process Automation with CA EEM. That is, register the configured "EEM Application Name" value with CA EEM. The registration process generates new CA Process Automation certificates.

Result: Certificates that CA Process Automation uses when invoking the CA EEM SDK Release 12.51 match the longer key lengths used by CA EEM.

See Example Scenario: Configure the Existing Installation to Regenerate CA Process Automation Certificates (see page 174).

Configure CA EEM to Permit Referenced Users to Log in with an Email Name

1. CA Process Automation Release 4.2 is installed with CA EEM using a referenced user store. The referenced user store is configured as Multiple Active Directories.
2. During CA Process Automation installation, you define which AD to use as the Default Active Directory.

   Referenced users belonging to the default AD can log in to CA Process Automation with their unqualified user name and password.
3. Without the next step, CA EEM permits referenced users in other domains to log in with their principal name (*domain**username)* and password.
4. Configure CA EEM to permit referenced users to log in with their email name (see page 145).

Result: Users who are not in the configured default AD domain can log in with their principal name and password, where both of the following formats for the principal name are supported:

username@*domain*

*domain**username*

Summary of Register Application with CA EEM

- If you select the Register Application with CA EEM check box and this is not a new installation, click **Register**. You are prompted for whether to upgrade the CA Process Automation application.
  - Select Yes to upgrade to a new release.
  - Select Yes to generate new CA Process Automation certificates as part of the "configure existing installation" process.
  - Select No if you are reinstalling the same release and you do not want to regenerate certificates.

Enable Secure Communications for an Existing CA Process Automation System

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. Specify secure communication in one of the following ways, depending on your installation method:
   - If you reinstall the Domain Orchestrator interactively (Install the Domain Orchestrator (see page 111)), select Support Secure Communication.
   - If you create a response file for unattended Domain Orchestrator Installation, set the isSecure variable to true to enable secure (HTTPS) communications:
     `isSecure=true`
2. Enable secure communication by agents in one of the following ways, based on their configuration.
   - Verify that agents configured to use deprecated communication are automatically restarted. (Deprecated communication is the default setting for existing agents.) Start any agents (see page 194) that were shut down before the reinstall.
   - Reinstall agents that were previously configured to use simplified communication. (Simplified communication is configured by clearing the Use Deprecated Communication check box during agent installation.) Reinstall agents as described in Installing an Agent (see page 183). Then start the agents (see page 194).

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

   Note: Existing SOAP attachments are accessible over HTTP only.

Chapter 8: Install Agents

This section contains the following topics:

Prerequisites to Installing Agents

Use the following guidelines to prepare for agent installation:

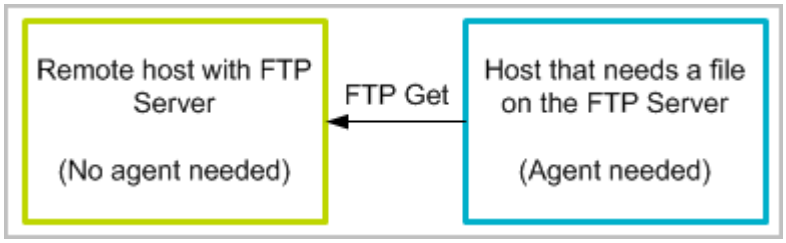
1. Identify hosts that need agents (see page 184).
2. Verify Java prerequisites for agents (see page 184).
3. Determine the port availability for the agent (see page 185) (only when using deprecated communication).
4. For secure environments (where Support Secure Communication was selected for Orchestrators), have at hand the Certificate Password that was set for all Orchestrators and Orchestrator nodes.

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



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

This step is only required for agents that use deprecated communication. Simplified communication uses standard ports for HTTP (port 80) and HTTPS (port 443).

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.

Browse to CA Process Automation and Log In

The URL you use to access CA Process Automation depends on whether the Domain Orchestrator is configured with one node (nonclustered) or multiple nodes (clustered). You can browse directly to a nonclustered CA Process Automation. For a clustered CA Process Automation, browse to the associated load balancer. You can reach all Orchestrators in the domain by launching the URL to the Domain Orchestrator or to the load balancer for the Domain Orchestrator.

Follow these steps:

1. Browse the CA Process Automation.

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

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

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

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

   The CA Process Automation login page opens.

2. Enter the credentials from your user account.

   Note: If CA EEM is configured to reference users from multiple Microsoft Active Directories and CA Process Automation does not accept your unqualified user name, enter your principal name. One format for a principal name is *domain_name**user_name*.

3. Click Log In.

   CA Process Automation opens. The Home tab displays.

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.

   A dialog appears showing the progress for downloading the application.
4. 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.

   All platforms support jre6; Windows supports jre6 and jre7.

   See the following example path for the Windows platform:

   ```
   C:\Program Files\Java\jdk1.7.0_45
   ```
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) Do not create a Start menu folder.
12. Examine the Domain URL. This is the URL from which you launched the agent installation. Click Next.

13. If the domain is secured (Support Secure Communication was selected during the installation of the Domain Orchestrator), provide the same Certificate Password that was used to install the Domain Orchestrator (and other Orchestrators).
14. Complete the General Properties page and then click Next.
    a. Enter the agent host name for Agent Host. This name identifies the host from which you started the installation.
    b. Change or accept the default Display Name, the host name.
    c. If you launched the agent installation from a Windows host, select Install as Windows Service.
    d. To force a new connection for each communication from an Orchestrator to an agent, select Use deprecated communication.

       We recommend that you leave this check box *cleared*. Simplified communications, the default, is preferred because it uses one persistent connection.
    e. If you selected Use deprecated communications, accept 7003 as the Agent Port unless this port is used. If the default port is used, enter an unused port number such as 57003 as the port on which the agent listens for communication with Orchestrators.

       Note: If deprecated communication is not used, then Orchestrators use a web-socket connection (established by agents) to communicate to agents. Orchestrators use port 80 to communicate with agents over HTTP. Orchestrators use port 443 to communicate with agents over HTTPS.
    f. Select Start Agent after Installation.

       Starting the agent lets you view the active agent and continue with the agent configuration.
15. 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.
16. Complete the setting in one of the following ways.
    - To run Windows PowerShell scripts through this agent:
      a. Select the Set PowerShell Execution Policy check box.
      b. Browse to the PowerShell host location if different from the displayed default.
      c. Click Next.
    - If you do not use Windows PowerShell, click Next.

    The Agent installation starts.
17. Click Finish.

18. (Windows only) Start the agent service. Click Start, Programs, CA, CA Process Automation Agent, Start Agent service.
19. Click the Configuration Browser palette on the Configuration tab.
20. Click Refresh. (Or, log out and log back in.)
21. Expand Agents and verify that your agent name is listed.

    Note: To use the agent host as a target, configure a touchpoint. To use the agent host as a gateway to a remote host, configure a proxy touchpoint.

More Information

About Agent Communication (see page 171)

Perform an 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 in 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

   The media folder includes the following files:

   - AgentInstaller
   - AgentInstaller.sh
   - AgentInstaller_64
   - AgentInstaller-hpux.sh
   - CA_PAM_Agent_unix.sh
   - CA_PAM_Agent_windows_32
   - CA_PAM_Agent_windows_64
4. Locate two files for your operating system:
   - Windows 32-bit: AgentInstaller.bat and CA_PAM_Agent_windows_32.exe
   - Windows 64-bit: AgentInstaller_64.bat and CA_PAM_Agent_windows_64.exe
   - UNIX and Linux: Agent Install.sh and CA_PAM_Agent_unix.sh
   - HP-UX: AgentInstaller-hpux.sh and CA_PAM_Agent_unix.sh
5. Copy both files for your operating system into a directory on the host where you want to install the agent.
6. Log on to the host where you want to install the agent and you navigate to the directory where you copied the agent installer and wrapper files.
7. (Optional) Run the agent installer without arguments to display help.
8. 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-VacceptLicens
   e=true
   ```

   ```
   -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.

VcertPassword=*value*

Specifies the certificate password as configured in the Domain Orchestrator. This value is required when you are using SSL and/or are working in Secure mode.

VisLookUpDNSForIP=*boolean*

Set the value to true to look up the agent host name from DNS.

jetty.ssl.ciphers=*value*

The list of comma-separated ciphers that must be used during Domain Orchestrator-agent communication.

-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.

-VdeprecatedComms=*boolean*

Specifies the communication mode (see page 171). Set the value to true to support the deprecated mode of communication. Set the value to false to support the new mode of communication.

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 192).
- 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 193).
- Agents that are installed with CA Process Automation Release 4.2 use simplified communication, by default. See the *Content Administrator Guide* for how to configure agents to use deprecated communication, if you are using an Apache load balancer. If you just upgraded to CA Process Automation Release 4.2, see the topic on how to configure existing agents to use simplified communication.

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 you start and stop an agent depends on the operating system that the host on which the agent is installed uses.

- Start an Agent (see page 194).
- Stop an Agent (see page 195).

Start an Agent

Use the agent start or restart method for the operating system on the host containing the agent.

Start or restart an agent on a Microsoft Windows host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a Windows operating system.

Follow these steps:

1. Log on to Windows host on which an agent is installed.
2. From the Start menu, select Programs, CA, CA Process Automation Agent, Start Agent Service.
3. Log off the host.

Start or restart an agent on a Linux host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a UNIX or Linux operating system.

Follow these steps:

1. Log on to the UNIX or Linux host on which an agent is installed.
2. Change directories to:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Run the following command:

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

   The agent restarts.

Stop an Agent

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

Stop an agent on a Microsoft Windows host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a Windows operating system.

Follow these steps:

1. Log on to Windows host on which an agent is installed.
2. From the Start menu, select Programs, CA, CA Process Automation Agent, Stop Agent Service.
3. Log off the host.

Stop an agent on a Linux host

The following steps apply to any agent in your CA Process Automation domain that resides on a host with a UNIX or Linux operating system.

Follow these steps:

1. Log on to the UNIX or Linux host on which an agent is installed.
2. Change directories to:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Run the following command:

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

   The agent stops running.

Offline Configuration of Agents to a Different Domain

In previous releases, the Domain Orchestrator had to be up and running to install a CA Process Automation Agent. In this release, you can create an agent image from the existing installed agent. Use the agent image that you create to install agents in an offline mode to the same domain or a different domain. In addition to installing new agents, you can also configure the existing agents to a different domain.

The procedure to configure agents to a different domain in an offline mode is as follows:

1. Create Agent Image (see page 196)
2. Configure Agents to a Different Domain (see page 197)

Create Agent Image

You use a batch (*ConfigureAgent.bat*) file or a shell (*ConfigureAgent.sh*) file to configure the CA Process Automation agent image to a new domain.

Follow these steps:

1. Install the Domain Orchestrator (see page 111) on the host system.
2. Install an Agent Interactively (see page 186).
3. Start an Agent (see page 194).

   The CA Process Automation agent is up and running.
4. Stop an agent (see page 195).

   The CA Process Automation agent stops.
5. Create a zip file of the agent folder. The zip file is termed as an “agent image”.

   Note: You can configure agents to a different domain based on the following agent images:

   - For agent images of secure agents, you can configure agents to a secure domain only.
   - For agent images of unsecure agents, you can configure agents to an unsecure domain only.
   - For the agent images of the agents that use simplified communication, you can configure agents to use only simplified communication.

     Note: You can make the agents that are configured to use simplified communication to use deprecated communication. For more information, see the Change Agent Configuration from Simplified to Deprecated Communication (see page 199).

Example

After you install a CA Process Automation agent, the agent installation wizard creates a folder at the following location: <*Agent_Installation_Location*>/PAMAgent. You need to create a zip file (*PAMAgent.zip*) of the PAMAgent folder.

Use the agent image to Configure Agents to a Different Domain (see page 197) (or a new domain).

Configure Agents to a Different Domain

You can configure the agents to a different domain in the following two operating environments:

- Configure Agents in Windows (see page 197)
- Configure Agents in Unix (see page 198)

Configure Agents in Windows

You can configure agents to a different domain in Windows using the *ConfigureAgent.bat* script file.

Follow these steps:

1. Unzip the zip file (*PAMAgent.zip*) of the agent folder (PAMAgent folder).
2. Access the *ConfigureAgent.bat* file
3. (Optional) Run the *ConfigureAgent.bat* file without arguments to display help.
4. Use the following command-line arguments with the agent installer:
   `ConfigureAgent.bat domainUrl=<value> certPassword=<value> [options]`

   domainUrl=*value*

   Specifies the URL of the domain server.

   For example, domainURL=*http://domainserver.company.com:8080/*

   Note: Do not append the context '*itpam*' to the domainUrl.

   certPassword=*value*

   Defines the certificate password that is configured in the Domain. This value is applicable for only secured mode of communication.

   listeningAddress=*value*

   Specifies the address of the agent host name.
5. Verify that the agent is configured to a new domain by the following message:

   The Agent is successfully configured with the Domain Orchestrator URL “domainUrl”.

Configure Agents in Unix and Linux

You can configure agents to a different domain in Unix and Linux using the *ConfigureAgent.sh* script file.

Follow these steps:

1. Unzip the zip file (*PAMAgent.zip*) of the agent folder (PAMAgent folder).
2. Access the *ConfigureAgent.sh* file
3. (Optional) Run the *ConfigureAgent.sh* file without arguments to display help.
4. Use the following command-line arguments with the agent installer:
   `ConfigureAgent.sh domainUrl=<value> certPassword=<value> [options]`

   domainUrl=*value*

   Specifies the URL of the domain server.

   For example, domainURL=*http://domainserver.company.com:8080/*

   Note: Do not append the context '*itpam*' to the domainUrl.

   certPassword=*value*

   Defines the certificate password that is configured in the Domain. This value is applicable for only secured mode of communication.

   listeningAddress=*value*

   Specifies the address of the agent host name.
5. Verify that the agent is configured to a new domain by the following message:

   The Agent is successfully configured with the Domain Orchestrator URL “domainUrl”.

Change Agent Configuration from Simplified to Deprecated Communication

If an agent is configured to use the simplified communication, you can configure the agent to use the deprecated communication.

Follow these steps:

1. Click the Configuration tab and expand Agents on the Configuration Browser palette.
2. Select the agent for which to switch communication and click Lock.
3. Select the Properties tab for the selected agent.
4. Check the Use Deprecated Communication check box.
5. Select the agent and click Unlock.
6. Click Yes on the Unsaved Data dialog to save the changes.

   The data of the agent is saved and the agent is configured to deprecated communication mode.

Chapter 9: Add 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. Use the same process for upgrading a node that you used for adding a node.

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 shares the same databases that were configured for the other existing nodes which are a part of the Domain Orchestrator cluster.

Before you install, 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 26).
   - Hardware Requirements (see page 28).
2. Verify that the host for this cluster node is in the same subnet as other existing nodes which are a part of the Domain Orchestrator.
3. Verify that the host for this cluster node is in the same timezone as other existing nodes which are a part of the 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 93).

5. If the host for this cluster node is running a recent version of a Windows operating system, review the User Account Control option (in the Control Panel, User Accounts). If this option is turned on, clear the check box and reboot this server.
6. 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 53).
7. 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 behavior. The entry resembles the following information:

      ```
      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.

8. If the first node of the Domain Orchestrator was configured with an NGINX load balancer, add this node (node2) to the load balancer.

   a. Navigate to and open the pam-server.conf file.

   b. Find the #Define node2 line. (The node1 data refers to the first Domain Orchestrator node; skip sections that refer to node1)

      Note: The *node2_hostname* is the IP address or DNS name of the host where the node2 is installed. The *jetty_server_port* is the "Server Port" value supplied during installation of the first node of the Domain Orchestrator. Enter 80 for simplified communication or enter 7003 for deprecated communication.

   c. Create the following entries in pam-server.conf to define both node1 and the new node, node2:

```
// node1 is the worker node name
upstream node1{
  # Define node1
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
// node2 is the worker node name
upstream node2{
  # Define node2
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

d. Inside server tag create following entries for both node1 and the new node, node2:

```
Server{

...
    location = /ws {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/ {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/node1 {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location /ws/node1/ {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/node2 {
               // node2 is the upstream name provided above
                proxy_pass http://node2;
               }
    location /ws/node2/ {
               // node2 is the upstream name provided above
               proxy_pass http://node2;
               }
}
```

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 201). 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 the Domain Orchestrator URL and log in.

   `https://`*`Load-Balancer-hostname`*`:8443/itpam`

   `http://`*`Load-Balancer-hostname`*`:8080/itpam`
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. Accept the license agreement, and click Next.
9. Specify the destination directory to install the Orchestrator node, 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.

    The Completing the CA Process Automation Setup Wizard for prerequisites displays a Use Domain check box and a path. Verify that this check box is selected. 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.
11. Click Finish to launch the installation of the cluster node for the Domain Orchestrator.
12. On the Welcome screen, click Next.
13. Accept the license agreement, and click Next.
14. 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.

15. Complete the Configuration Screen, and click Next.

    Orchestrator

    Specifies the Orchestrator to which the cluster node is to be added. The Orchestrator selected from the drop down list must be configured with a Public Host Name that specifies the FQDN of the server where the load balancer is installed.

    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 first installation of the Domain Orchestrator is node1. For the second node, type **node2.**

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

    Certificate Password

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

18. 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.

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

    The cluster node for the Domain Orchestrator is installed.

Synchronize Time for a Cluster Node

All cluster nodes for any Orchestrator must have the exact same clock time, which is synchronized with a standard external time server. 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 all additional cluster nodes as follows:
  1. Verify the accuracy of the time of all cluster nodes.
  2. Run the appropriate OS command on each cluster nodes to synchronize the time of all cluster nodes.

Chapter 10: Install 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 26).
   - Hardware Requirements (see page 28).
2. Verify that the host for the Orchestrator has a supported JDK, and if missing, download it.

   See JDK Prerequisites (see page 93).

3. Have at hand the certificate password used for the Domain Orchestrator. This password controls access to the keys used to encrypt passwords and other critical data.

   Important! You cannot successfully install another Orchestrator without this password.

4. Identify the type of databases for the CA Process Automation data stores. Consider the following factors:

   - Each Orchestrator must have its own Runtime data store.
   - An Orchestrator can share the Library data store of the Domain Orchestrator or have its own Library data store. All Orchestrators in the same environment typically share the same Library data store
   - Typically, all Orchestrators in the Domain use the Reporting data store created for the Domain Orchestrator.

5. Prepare the database servers.

   - See Database Server Prerequisites (see page 86).
   - 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 26).
     - Hardware Requirements (see page 28).

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

   Note: We recommend a hardware load balancer. See F5 Load Balancer Prerequisites (see page 52). If this is not possible, we recommend NGINX as the software load balancer of choice. NGINX for UNIX is highly scalable. NGINX for Windows can support up to 300 agents using simplified communication. See NGINX Load Balancer Prerequisites.

7. If you plan to cluster this Orchestrator using NGINX, take the following additional steps:

   a. Navigate to and open the pam-server.conf file.

   b. Find the #Define node1 line. (The node1 data refers to the Orchestrator node that is installed first.)

   c. Insert the following, where the *jetty_server_port* is the value configured at installation for Server Port. Typically, the values are 80 for simplified communication or 7003 if agents that connect to this Orchestrator use deprecated communication.

```
// node1 is the worker node name
upstream node1{
  # Define node1
  server node1_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

   d. Inside Server tag create following entries:

```
Server{
       location = /ws {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location = /ws/ {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location = /ws/node1 {
                 // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location /ws/node1/ {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
...
                }
}
```

8. 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.
9. 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 that hosts the databases you plan to use for the Runtime data store and optionally, a separate Repository (or Library) data store.

Install an Orchestrator

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

Before you use the following procedure, complete the prerequisites to installing an Orchestrator (see page 209). For example, verify that you have a JDK installed.

Use the following process to install an Orchestrator or to upgrade an existing Orchestrator.

Follow these steps:

1. Log in to the server on which to install the new Orchestrator.
2. Browse to CA Process Automation and log in (see page 186) with administrator credentials. For example, log in as a member of the PAMAdmins group.
3. Click the Configuration tab and select the Installation palette.
4. Click the prerequisites link and verify that all prerequisites have been met.
5. Click Install Orchestrator.

   If you use the Firefox web browser, open it with Java Web Start Launcher (the default).

   If necessary, install the required certificate as instructed. The application downloads. The Language Selection dialog may appear in the system tray.
6. Select a language and click OK.

   The Welcome to the CA Process Automation Third-Party Installer Setup wizard page appears.
7. Click Next.

8. Accept the licensing agreement, and click Next.
9. Accept the default installation directory (install_dir) or change it, and click Next.
10. Click Next on the Prerequisites for CA Process Automation Installation page.

    The Installing JBoss page shows the progress of installing jboss-5.1.
11. Specify JDBC jars for installation in one of the following ways:
    - Leave the Use Domain check box selected and click Next. This specifies to use the JDBC jars that the Domain Orchestrator installation configured.
    - Complete the following procedure:
        a. Clear the Use Domain check box.
        b. Click Add Files.
        c. Select the database server type.
        d. Click Browse and navigate to the JDBC JAR file for the selected server type.
        e. Click Next.
12. On the confirmation screen, click Next.
13. Click Finish to advance to the CA Process Automation installer.
14. Click Next on the Welcome screen.
15. Accept the license agreement and click Next.
16. Take one of the following actions on the Java Home Directory page:
    - Click Next to accept the default.
    - Browse to the JDK location and click Next.
17. View the Domain URL, and click Next.

18. If you are not using Single Sign-on a load balancer, click Next and skip the following step.
19. Complete this page and click Next.

Configure Single Sign-on (SSO)

Specifies whether you are using CA SiteMinder with SSO, where the default is cleared. Selecting this option enables these fields:

- SSO Authentication Type (Header)
- SSO Authentication Parameter (sm-user)
- Type of server (New Orchestrator)

Configure Load Balancer

Specifies whether to install this Orchestrator so it can cluster.

Selected

Indicates that a load balancer is configured for this Orchestrator.

Cleared

Indicates that no load balancer is configured for this Orchestrator.

Load Balancer Worker Node

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

Note: For nodes other than node1 (for example, node 2), see:

- Adding a Node to the Domain Orchestrator (see page 201).
- Adding a Node to an Additional Orchestrator (see page 219).

Public Host Name

Specifies the public host name for the Apache server, NGINX server, or the F5 server. For example:

loadbalancerhost.*mycompany*.com

- Set this field to the FQDN of the Apache, F5, or NGINX load balancer if you selected the Configure Load Balancer check box.

Public Host Port Number

If Support Secure Communication is cleared, this field specifies the HTTP port for the Public Host.

Default

80

Public Host Secure Port

If Support Secure Communication is selected, this field specifies the HTTPS port for the Public Host.

Default

443

Support Secure Communication

Specifies whether the Public Host uses HTTPS for secure communication.

Selected

The Public Host uses HTTPS for secure communication.

Cleared

The Public Host does not use HTTPS for secure communication; instead, it uses HTTP for basic communication.

20. View the Company Name, and click Next.
21. Enter the certificate password that the Domain Orchestrator uses, and click Next.

    If this certificate password is lost or forgotten, you must reinstall all Orchestrators in the CA Process Automation system and specify this certificate password, beginning with the Domain Orchestrator.
22. Specify Start Menu Folder preferences and click Next.
23. Enter the General Properties for the Orchestrator, and click Next.

    Server Host

    Specifies the FQDN of this Orchestrator.

    Display Name

    Specifies the name that the Configuration Browser displays for this Orchestrator.

    - If you do not configure a load balancer, the Display Name is the Server Host name.
    - If you configure a load balancer, the Display Name is the FQDN of the server that hosts the load balancer.
24. Accept the default or set the temporary directory in which to run scripts, then click Next.
25. Set the PowerShell run policy and click Next.

26. Enter the Repository database settings for this Orchestrator in one of the following ways:
    - To share the Repository (Library) data store that the Domain Orchestrator uses, complete the following procedure:
        a. Enter the same information that you configured for the Domain Orchestrator.
        b. Click Test Database Settings.
        c. Click Next.
    - To create a separate Repository (Library) data store for this Orchestrator, complete the following procedure:
        a. For MS SQL or MySQL, enter a unique name for the new database in the Repository database field.
        b. For Oracle, enter an existing schema in the User Name field that is different from the schema defined for the Repository data store used by the Domain Orchestrator.
        c. For MS SQL or MySQL, click Create Database to create the new database.
        d. Click Test Database Settings
        e. Click Next.
27. Enter the Runtime database settings. Each Orchestrator requires a separate Runtime data store.
    a. If the new Runtime data store resides in the same database instance as the Repository data store for this Orchestrator, click Copy from the Main Repository.
    b. If the database instance you specify hosts other Runtime data stores, proceed based on your database type.
        – For MS SQL or MySQL, enter a unique name for the new database in the Runtime database field.
        – For Oracle, create a new schema, if needed, and specify the schema in the User Name field.
    c. For MS SQL and MySQL, click Create Database.
    d. Click Test Database Settings.
    e. Click Next.
28. View Reporting Database Settings and click Next. All Orchestrators in the Domain share the same Reporting data store.
29. 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 108).
3. Configure firewalls for bi-directional communication (see page 142).
4. If you installed the Domain Orchestrator on a server with the HP-UX operating system, perform additional configuration steps on HP-UX.
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 11: Add a Node to an Additional Orchestrator

After you install an additional Orchestrator, you can extend its capacity and provide failover capability by adding a cluster node. If any node fails, other node takes the control. You can use an interactive or unattended installation to 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 shares the same data stores that were configured for the other existing nodes which are a part of the Orchestrator cluster.

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 26).
   - Hardware Requirements (see page 28).
2. Verify that the host for this cluster node is in the same subnet as the other existing nodes which are a part of the Orchestrator.
3. Verify that the host for this cluster node is in the same timezone as the other existing nodes which are a part of the Orchestrator.
4. Verify that the host for this cluster node has a supported JDK, and if missing, download it.

   See JDK Prerequisites (see page 93).
5. If the host for this cluster node is running a recent version of a Windows operating system, review the User Account Control option (in the Control Panel, User Accounts). If this option is turned on, clear the check box and reboot this server.

6. 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 53).

   If this is the first node, see F5 Load Balancer Prerequisites (see page 52).

7. 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 behavior. 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.

8. If the Orchestrator was configured with an NGINX load balancer, add this node to the load balancer.

   a. Navigate to and open the pam-server.conf file.

   b. Find the #Define node2 line. (The node1 data refers to the first Orchestrator node; skip sections that refer to node1.)

   c. Insert the following

```
# Define node2
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

   Note: The jetty server port is the "Server Port" value supplied during installation of the first node of the Domain Orchestrator. Enter 80 for simplified communication or enter 7003 for deprecated communication.

   Inside server tag create following entries:

```
Server{
     location = /ws {
...
                  // node2 is the upstream name provided above
                  proxy_pass http://node2;
                  }
     location /ws/node2/ {
                  // node2 is the upstream name provided above
                  proxy_pass http://node2;
                  }
}
```

Install a Cluster Node for an Orchestrator

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

Verify the completion of prerequisites to installing a cluster node for an Orchestrator (see page 219). Then, install the cluster node. This same procedure is used when upgrading a cluster node to a new release.

Follow these steps:

1. Log in to the server where you plan to install this cluster node for an additional Orchestrator.
2. Browse to the Orchestrator to which you want to add the cluster node and log in.

   `https://Load-balancer-hostname:8443/itpam`

   `http://Load-balancer-hostname:8080/itpam`

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. Accept the license agreement, and 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.

   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.
10. Click Finish to move on to the CA Process Automation installer.
11. On the Welcome screen, click Next.
12. Accept the license agreement, and click Next.
13. 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.

14. Complete the Configuration Screen, and click Next.

    Orchestrator

    Specifies the Orchestrator to which the cluster node is to be added. The Orchestrator selected from the drop down list must be configured with a Public Host Name that specifies the FQDN of the server where the load balancer is installed.

    Load Balancer Worker Node

    Specifies the node name.

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

    For Apache, 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

15. View the Company Name, and click Next.
16. Enter the *same* certificate password that was entered during the installation of the Domain Orchestrator, and click Next.
17. Specify a Start Menu Folder, and click Next.
18. Enter the General Properties for the Orchestrator, and click Next.

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

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

    The cluster node for the selected Orchestrator is installed.

Synchronize Time for a Cluster Node

All cluster nodes for any Orchestrator must have the exact same clock time, which is synchronized with a standard external time server. 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 all additional cluster nodes as follows:
  1. Verify the accuracy of the time of all cluster nodes.
  2. Run the appropriate OS command on each cluster nodes to synchronize the time of all cluster nodes.

Chapter 12: CA Process Automation Tuning

This section contains the following topics:

How to Improve Performance of CA Process Automation

As you approach how to boost or enhance performance, consider the following guidelines:

- Convert each standalone Orchestrator to a cluster.

  Adding a second node can improve performance by up to 80%. The improvement you achieve depends on many variables, including the CA Process Automation content being run.

- Content
  - Global Datasets

    Minimize references to global datasets, as access to them is serialized. That is, only one object can access a dataset at a time. This guideline applies to writes (not reads).

    The best practice is to make a Process-level copy of the required data and then refer to that process dataset.

  - Inline processes

    Limit the use of launching processes inline to cases in which both of the following are true:

    - There are fewer than 10 operators in the inline process.
    - The inline process is not called inside a loop.

- CPUs
  - Monitor CPU usage on all Orchestrator nodes to determine which nodes could best benefit from additional CPUs or cores.
  - Add more CPUs or cores, as needed.
  - When running in a virtual environment, dedicate the CPUs to the CA Process Automation VMs.

- Memory
  - When running in a virtual environment, dedicate the RAM to the CA Process Automation VMs.
  - Monitor the process memory usage on all Orchestrator nodes to determine whether additional RAM is needed.
- VM server optimization

  Refer to your VM server vendor for instructions on how to boost performance.
- Database optimization and maintenance

  Refer to the your database server vendor for instructions on how to boost and maintain the performance of the CA Process Automation database. Such instructions typically include database re-indexing, the updating of statistics, as well as the monitoring and maintenance of the file system on which data is stored.
- Turn off all unneeded features
  - Catalyst

    If you are not using Catalyst connectors, find the following value in the OasisConfig.properties and change it from true to false:

    ```
    # enable connector
    ucf.connector.enabled=true
    ```
  - Reporting

    If you are not using Reporting, insert the following key value pair into the OasisConfig.properties file. Changes to this file go into effect when the CA Process Automation service is restarted.

    ```
    oasis.disable.reporting.manager=true
    ```
- VMware

  If using VMware, change the virtual NIC from E1000 to VMXNET3. This change typically improves both performance and reliability.

Tuning CA Process Automation by Editing Configuration Files

JVM Tuning

Consider doing JVM tuning.

Follow these steps:

1. Log in to the server where an Orchestrator is installed.
2. Navigate to the following folder:

   install_dir/server/c2o/bin/
3. Open the following file:

   c2osvcw.conf
4. Edit the following parameters as shown:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Note: The wrapper.java.initmemory and the wrapper.java.maxmemory values must be identical. If additional memory is required and available on the server, these values can be changed.
5. Save the updated c2osvcw.conf file.

JBOSS JMS and Database Pools Tuning

Consider updating default values for JBOSS JMS and Database pools.

Follow these steps:

1. Log in to the server where an Orchestrator is installed.
2. Navigate to the following folder:

   install_dir/server/c2o/conf/
3. Open the following file:

   install_dir/server/c2o/conf/standardjboss.xml

4. Edit the following parameter as shown:
   - Under <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Under <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

5. Save the updated standardjboss.xml file.

Appendix A: Use CA 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 Secure Proxy Server (CA SiteMinder SPS) installed and configured with Policy Server.

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 ApacheDefaultSettings.
   - 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

- /newWelcome.jsp
- /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*.

Configure CA SiteMinder Secure Proxy Server for CA Process Automation

To configure CA SiteMinder Secure Proxy Server (CA SiteMinder SPS) for CA Process Automation, access the CA SiteMinder Secure Proxy Server Administrative UI. For more information, see the *CA SiteMinder Secure Proxy Server Administration Guide*.

Important! Before you configure CA SiteMinder SPS 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.

Follow these steps::

1. Install CA SiteMinder SPS. For more information, see *CA SiteMinder Secure Proxy Server Administration Guide.*
2. Configure the CA SiteMinder Policy Server Objects (see page 230)
3. Locate the proxyrules.xml file of the CA SiteMinder SPS in the following location:

   $SecureProxyInstallLoc/proxy-engine/conf
4. Add the following rules within the <nete:proxyrules> tag:

   Note: Provide the appropriate rules that are based on the setup environment as follows:

   - For a cluster environment, the request is forwarded to the loadbalancer. You provide the following rule with loadbalancer details: <nete:forward>http://< *loadbalancer hostname:port* >$0</nete:forward>
   - For Standalone domain, the request is forwarded to a standalone domain. You provide the following rule with loadbalancer details: <nete:forward>http://<*standalone domain hostname*:8080>$0</nete:forward>

   Non-Secure Communications using CA SiteMinder SPS:

   For a cluster environment in a non-secure proxy server environment, add the following rule:

```
  <nete:cond criteria="beginswith" type="uri">
              <nete:case value="/itpam/">
          <nete:forward>http:// <loadbalancer
hostname:port>$0</nete:forward>
      </nete:case>
      <nete:case value="/itpam">
        <nete:forward>http:// <loadbalancer
hostname:port>/itpam/</nete:forward>
      </nete:case>
   <nete:case value="/birt">
       <nete:forward>http:// <loadbalancer
hostname:port>$0</nete:forward>
      </nete:case>
          <nete:case value="/ucf/BrokerService">
          <nete:forward>http://<loadbalancerhost>:<loadbalancer
port for REST services>$0</nete:forward>
       </nete:case>
       <nete:case value="/node/rest/CA:00074_CA:00074:01">
       <nete:forward>http://<loadbalancerhost>:<lb port for REST
services>$0</nete:forward>
      </nete:case>
      <nete:default>
         <nete:forward>http://www.ca.com/</nete:forward>
      </nete:default>
  </nete:cond>
```

Note: You should define the loadbalancerhost name as a FQDN hostname. For example, *loadbalancer12 .ca.com* is a FQDN hostname.

Secure Communications using CA SiteMinder SPS:

Note: To configure CA SiteMinder SPS for secure communications, refer the *CA SiteMinder Secure Proxy Server Administration Guide*.

For a cluster environment in a secure environment, configure CA SiteMinder SPS as follows:

a. Add the following rule:

```
  <nete:cond criteria="beginswith" type="uri">
              <nete:case value="/itpam/">
          <nete:forward>https:// <loadbalancer
hostname:port>$0</nete:forward>
      </nete:case>
      <nete:case value="/itpam">
        <nete:forward>https:// <loadbalancer
hostname:port>/itpam/</nete:forward>
      </nete:case>
   <nete:case value="/birt">
       <nete:forward>https:// <loadbalancer
hostname:port>$0</nete:forward>
      </nete:case>
          <nete:case value="/ucf/BrokerService">

   <nete:forward>https://<loadbalancerhost>:<loadbalancer port
for REST services>$0</nete:forward>
       </nete:case>
       <nete:case value="/node/rest/CA:00074_CA:00074:01">
       <nete:forward>https://<loadbalancerhost>:<lb port for
REST services>$0</nete:forward>
      </nete:case>
      <nete:default>
         <nete:forward>http://www.ca.com/</nete:forward>
      </nete:default>
  </nete:cond>
```

Note: You should define the loadbalancerhost name as a FQDN hostname. For example, *loadbalancer12 .ca.com* is a FQDN hostname.

b. If CA Process Automation is in secure mode, configure CA SiteMinder SPS in secure mode. To configure CA SiteMinder SPS in secure mode, see *CA SiteMinder Secure Proxy Server Administration Guide*.

c. For secure mode, you need to generate the CA Process Automation certificate. To generate the CA Process Automation certificate, see the Generate SSL Certificate Files (see page 37) section.

d. Copy the content of the CA Process Automation certificate (c2ocert.pem) and append the content to the certificate bundle file (ca-bundle.cert file) in the following location:

<*CA SiteMinder SPS Installation_dir*> \SSL\certs\ ca-bundle.cert

Note: When integrating SPS with a CA Process Automation cluster using an Apache load balancer in secure communication, add the Apache certificates to the SPS cert bundle.

5. Restart CA SiteMinder SPS.

Note: To use CA SiteMinder SPS with CA Process Automation, you configure the SSO details in the configuration screen during the CA Process Automation installation.

By default, CA Process Automation uses SSO Authentication Type as *Header* and Authentication Parameter as *sm_user*. CA Process Automation Install and Upgrade does not support CA SiteMinder Web Agent on Apache and IIS. CA Process Automation Install and upgrade uses only CA SiteMinder SPS. When you upgrade CA Process Automation, you provide the CA SiteMinder SPS details to use SSO instead of Web Agent on Apache. For more information, see Install the Domain Orchestrator (see page 111) section.

Enable Logout in CA Process Automation for SSO

You can allow Single Sign-on logout in CA Process Automation.

Follow these steps:

1. Navigate to the following location:

   `install_dir/server/c2o/.config`

2. Double-click to open OasisConfig.properties file.
3. Modify ALLOW_SSO_LOGOUT to true.

Appendix B: Ports Used by CA Process Automation

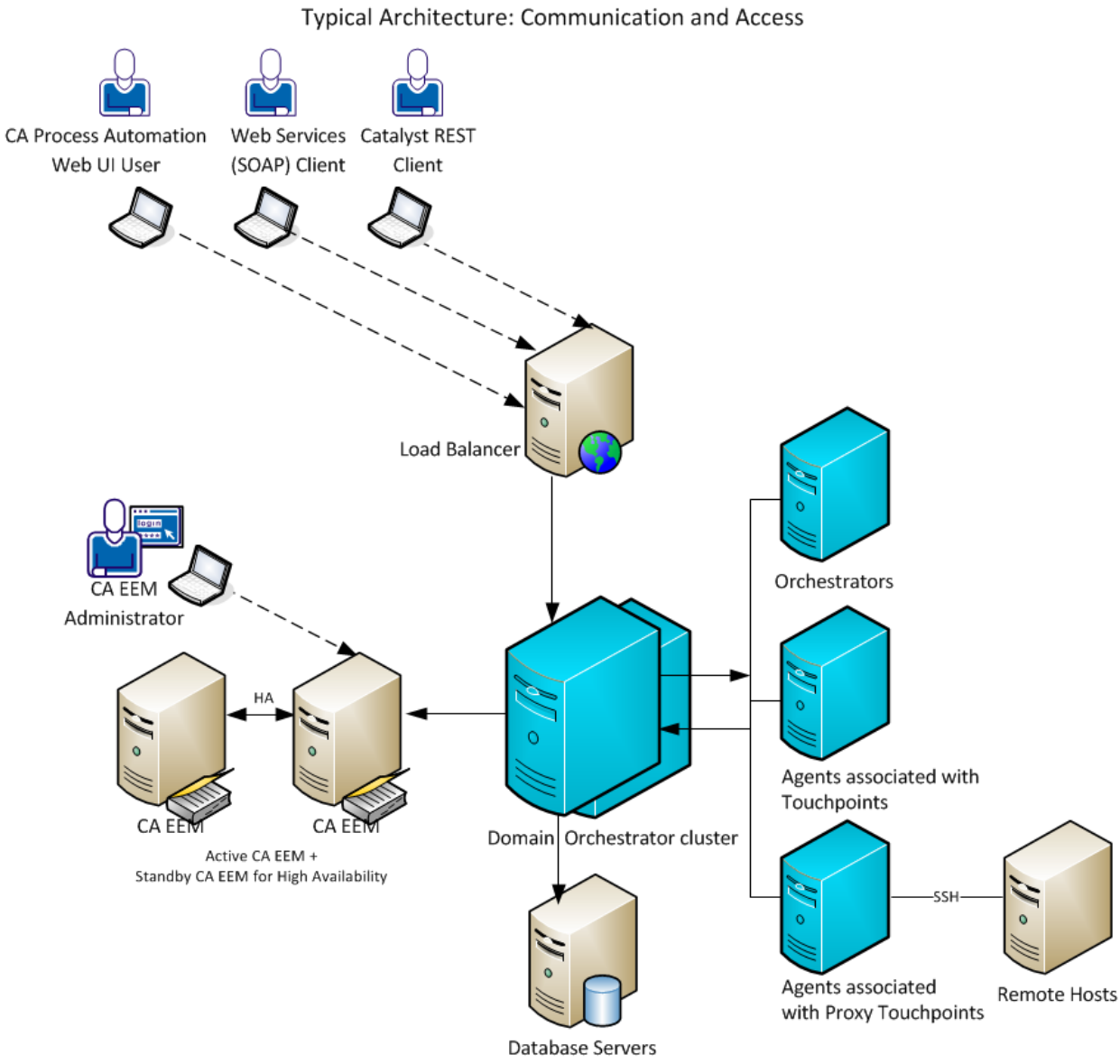
This appendix is composed of tables that describe in detail the port usage of the various CA Process Automation components. These tables are comprehensive and contain duplication in order to provide a complete picture for each component.

For an illustration of how components communicate, see Communication in a Typical Architecture (see page 236).

This section contains the following topics:

Communication in a Typical Architecture

The following diagram shows the relationships among components referenced in this appendix.



Note: The following tables contain a "Configuration" column that identifies where listener ports can be configured.

More information:

Planning the Locations of Supporting Components (see page 85)

Ports Used by CA EEM

The following tables provide an overview of the ports used for communications from and to CA Embedded Entitlements Manager (CA EEM).

Communication from CA EEM

From	Port	To	Default Listening Port	Protocol	Configuration	Description
CA EEM	Any	CA EEM	509	TCP	CA EEM configuration	Used by CA EEM iTechPoz when CA EEM is configured as an HA cluster.
CA EEM	Any	CA EEM	1684	TCP	CA EEM configuration	Used by CA EEM iTechPoz Router when CA EEM is configured as an HA cluster (CA EEM 8.4 only)
CA EEM	Any	CA EEM	5250	TCP	CA EEM configuration	Used by CA EEM iGateway when CA EEM is configured as an HA cluster

Communication to CA EEM

From	Port	To	Default Listening Port	Protocol	Configuration	Description
CA EEM	Any	CA EEM	509	TCP	CA EEM configuration	Used by CA EEM iTechPoz when CA EEM is configured as an HA cluster.

From	Port	To	Default Listening Port	Protocol	Configuration	Description
CA EEM	Any	CA EEM	1684	TCP	CA EEM configuration	Used by CA EEM iTechPoz Router when CA EEM is configured as an HA cluster (CA EEM 8.4 only)
CA EEM	Any	CA EEM	5250	TCP	CA EEM configuration	Used by CA EEM iGateway when CA EEM is configured as an HA cluster
Orchestrator	Any	CA EEM	5250	TCP	CA EEM configuration	Used to validate credentials and permissions (authentication and authorization).
Web Browser (CA EEM Administrator)	Any	CA EEM	5250	TCP	CA EEM configuration	Web Browser accessing the CA EEM UI.

Ports Used by the Load Balancer

The following tables provide an overview of the ports that are used for communications from and to the configured load balancer. Supported load balancers include NGINX, Apache, and F5.

Communication from the Load Balancer

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Load Balancer	Any	Orchestrator	80	HTTP	Oasisconfig.properties	Load Balancer talks to Orchestrator on this port.
Load Balancer	Any	Orchestrator	443	HTTPS	Oasisconfig.properties	Load Balancer talks to secure Orchestrators on this port.

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Load Balancer	Any	Orchestrator	8080	HTTP	Oasisconfig.properties	Load Balancer talks to Orchestrator on this port.
Load Balancer	Any	Orchestrator	8443	HTTPS	Oasisconfig.properties	Load Balancer talks to secure Orchestrators on this port.
Load Balancer	Any	Orchestrator	8009	TCP/AJP	Oasisconfig.properties	Loadbalancer - AJP connector port between Load Balancer and Orchestrator. This port does not apply to NGINX.
Load Balancer	Any	Orchestrator	7000	HTTP	node0-config.xml	CA Process Automation Catalyst REST API port
Load Balancer	Any	Orchestrator	7443	HTTPS	node0-config.xml	CA Process Automation Catalyst REST API secure port

Communication to the Load Balancer

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Catalyst REST client	Any	Load Balancer	7000	HTTP	Apache: httpd-proxy.conf NGINX: pam-rest.conf F5: iRules config	CA Process Automation Catalyst container port
Catalyst REST client	Any	Load Balancer	7443	HTTPS	Apache: httpd-proxy.conf NGINX: pam-rest.conf F5: iRules config	CA Process Automation Catalyst container secure port
Agent	Any	Load Balancer	80	HTTP	Apache: httpd.conf NGINX: pam-server.conf F5: iRules Config	Load Balancer port for basic communication

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Agent	Any	Load Balancer	443	HTTPS	Apache: httpd-ssl.conf NGINX: secure-pam-server.conf F5: iRules config	Load Balancer port for secure communication
Web Browser (CA Process Automation Web UI user)	Any	Load Balancer	80	TCP	Apache: httpd.conf NGINX: pam-server.conf F5: iRules Config	Load Balancer port for basic communication
Web Browser (CA Process Automation Web UI user)	Any	Load Balancer	443	TCP	Apache: httpd.conf NGINX: secure-pam-server.conf F5: iRules	Load Balancer port for secure communication
Web Services (SOAP) client	Any	Load Balancer	80	TCP	Apache: httpd.conf NGINX: pam-server.conf F5: iRules Config	Load Balancer port for basic communication
Web Services (SOAP) client	Any	Load Balancer	443	TCP	Apache: httpd.conf NGINX: secure-pam-server.conf F5: iRules	Load Balancer port for secure communication

Ports Used by an Orchestrator

The following tables provide an overview of the ports used for communications, specifically:

- Communication from an Orchestrator to another component in a CA Process Automation system
- Communication between Orchestrators
- Communication to an Orchestrator from another component in a CA Process Automation system

Communication from an Orchestrator to another Component

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	CA EEM	5250	TCP	CA EEM configuration	Used to validate credentials and permissions (authentication and authorization)
Orchestrator	Any	Agent	7003	HTTP/ HTTPS	Specified during agent install or re-install	**Deprecated** Agent listens on this deprecated port when using the old mode of communication with Orchestrators
Orchestrator	Any	Microsoft SQL Database Server	1433	TCP	Microsoft SQL configured	The database port can be changed in the database server installation; 1433 is the default value.
Orchestrator	Any	MySQL Database Server	3306	TCP	MySQL configured	The database port can be changed in the database server installation; 3306 is the default value.

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Oracle Database Server	1521	TCP	Oracle configured Listener	The database port can be changed during Create Listener; 1521 is the default value for the Oracle Listener port. The database instance can be associated with a different listener. Refer to the Oracle configuration.

Communication between Domain Orchestrator and Non-Domain Orchestrator

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Non-Domain Orchestrator	7001	HTTP/ HTTPS	OasisConfig.properties	Port used for communication between Orchestrators.
Non-Domain Orchestrator	Any	Domain Orchestrator	8080	TCP	OasisConfig.Properties	Basic Orchestrator to Orchestrator communication
Non-Domain Orchestrator	Any	Domain Orchestrator	8443	TCP	OasisConfig.Properties	Secure Orchestrator to Orchestrator communication
Non-Domain Orchestrator	Any	Domain Orchestrator	80	TCP	OasisConfig.Properties	Basic Orchestrator to Orchestrator communication
Non-Domain Orchestrator	Any	Domain Orchestrator	443	TCP	OasisConfig.Properties	Secure Orchestrator to Orchestrator communication

Communication between Clustered Orchestrator Nodes

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Orchestrator	1090	TCP	OasisConfig.properties	JBoss Remoting port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	1098	TCP	OasisConfig.properties	JBoss RMI port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	1099	TCP	OasisConfig.properties	JBoss JNDI port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	1100	TCP	OasisConfig.properties	JBoss: HA_Java Naming and Directory Interface is used only between Orchestrators.
Orchestrator	Any	Orchestrator	1101	TCP	OasisConfig.properties	JBoss: HA-Java Remote Method Invocation is used only between Orchestrators.
Orchestrator	Any	Orchestrator	1102	UDP	OasisConfig.properties	JBoss: JNDI Autodiscovery service is used only between Orchestrators.
Orchestrator	Any	Orchestrator	3873	TCP	OasisConfig.properties	JBoss: EJB3 Remoting Connector is used only between Orchestrators.
Orchestrator	Any	Orchestrator	4444	TCP	OasisConfig.properties	JBoss RMI Server port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	4445	TCP	OasisConfig.properties	JBoss Pooled Invoker port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	4446	TCP	OasisConfig.properties	JBoss HA Pooled Invoker port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	4447	TCP	OasisConfig.properties	JBoss HA-RMI Server port is used only between Orchestrators.

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Orchestrator	4448	TCP	OasisConfig.properties	JBoss HA Pooled Invoker port is used only between Orchestrators
Orchestrator	Any	Orchestrator	4457	TCP	OasisConfig.properties	JBoss Messaging port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	4712	TCP	OasisConfig.properties	JBoss Transaction Status Recovery Manager port is used only between Orchestrators
Orchestrator	Any	Orchestrator	4713	TCP	OasisConfig.properties	JBoss Transaction Status Manager port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	7600	TCP	OasisConfig.properties	JBoss clustering port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	7900	TCP	OasisConfig.properties	JBoss clustering port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	7901	TCP	OasisConfig.properties	JBoss clustering port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	8083	TCP	OasisConfig.properties	JBoss RMI WebService port is used only between Orchestrators.
Orchestrator	Any	Orchestrator	61618	TCP	OasisConfig.properties	ActiveMQ messaging subsystem.

Note: CA Process Automation uses JBoss 5.1, which listens on a random set of dynamic ports in the range (49152-65535). The dynamic ports are required for various features, including cluster node communication. If CA Process Automation cannot communicate on these ports, functionality may be severely limited (for example, processes may become stuck).

CA recommends that nothing be placed between cluster nodes that could block communication. If a firewall is required, CA recommends that you open all TCP ports in both directions between the cluster nodes for the java.exe process that is associated with CA Process Automation.

Communication to a Clustered Orchestrator from another Component

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Load Balancer	Any	Orchestrator	8080	HTTP	Oasisconfig.properties	Load Balancer talks to Orchestrator on this port.
Load Balancer	Any	Orchestrator	8443	HTTPS	Oasisconfig.properties	Load Balancer talks to secure Orchestrators on this port.
Load Balancer	Any	Orchestrator	7000	HTTP	node0-config.xml	CA Process Automation Catalyst REST API port
Load Balancer	Any	Orchestrator	7443	HTTPS	node0-config.xml	CA Process Automation Catalyst REST API secure port
Load Balancer	Any	Orchestrator	8009	TCP/AJP	Oasisconfig.properties	Loadbalancer - AJP connector port between Load Balancer and Orchestrator. This port does not apply to NGINX.
Agent	Any	Orchestrator	8080	HTTP	OasisConfig.properties	Deprecated communications only
Agent	Any	Orchestrator	8443	HTTPS	OasisConfig.properties	Deprecated communications only
Agent	Any	Orchestrator	7001	HTTP/ HTTPS	OasisConfig.properties	Deprecated port

Communication to a Non-Clustered Orchestrator from another Component

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Orchestrator	443	HTTPS	Jetty	Web-socket connection established by agents
Agent	Any	Orchestrator	8080	HTTP	OasisConfig.properties	Deprecated communications only

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Agent	Any	Orchestrator	8443	HTTPS	OasisConfig.properties	Deprecated communications only
Agent	Any	Orchestrator	80	HTTP	OasisConfig.properties	Basic Server Port
Agent	Any	Orchestrator	443	HTTPS	OasisConfig.properties	Secure Server Port
Agent	Any	Orchestrator	7001	HTTP/ HTTPS	OasisConfig.properties	Deprecated port
Web Browser (CA Process Automation Web UI user)	Any	Orchestrator	8080	HTTP	OasisConfig.properties	Browser talks to Orchestrator on this port with basic communication.
Web Browser (CA Process Automation Web UI user)	Any	Orchestrator	8443	HTTPS	OasisConfig.properties	Browser talks to secure Orchestrators on this port.
Web Services (SOAP) client	Any	Orchestrator	8080	HTTP	OasisConfig.properties	Orchestrator SOAP API server
Web Services (SOAP) client	Any	Orchestrator	8443	HTTPS	OasisConfig.properties	Orchestrator SOAP API server (secure)

Ports Used by an Agent

The following tables provide an overview of the ports used for communications from and to a CA Process Automation agent.

Communication from an Agent

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Agent	Any	Orchestrator	8080	HTTP	OasisConfig.properties	Deprecated communications only.
Agent	Any	Orchestrator	8443	HTTPS	OasisConfig.properties	Deprecated communications only.

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Agent	Any	Load Balancer	80	HTTP	Apache: httpd.conf NGINX: pam-server.conf F5: iRules Config	Load Balancer port for basic communication
Agent	Any	Load Balancer	443	HTTPS	Apache: httpd-ssl.conf NGINX: secure-pam-server.conf F5: iRules config	Load Balancer port for secure communication
Agent	Any	Orchestrator	7001	HTTP/ HTTPS	OasisConfig.properties	Deprecated Server Port
Agent	Any	Orchestrator	80	HTTP	OasisConfig.properties	Basic Server Port
Agent	Any	Orchestrator	443	HTTPS	OasisConfig.properties	Secure Server Port
Agent	Any	Target Remote Host	22	TCP	Standard SSH port	Used for SSH communication with a proxy touchpoint or host group.

Communication to an Agent

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Agent	7003	HTTP/ HTTPS	Agent installation script	Agent formerly listened on this deprecated port for communication with Orchestrators.

Ports Used by Database Servers

The following table provides an overview of the ports used for communications to a Database server.

Communication to a Database Server

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Orchestrator	Any	Microsoft SQL Database Server	1433	TCP	Microsoft SQL configured	The database port can be changed in the database server installation; 1433 is the default value.
Orchestrator	Any	MySQL Database Server	3306	TCP	MySQL configured	The database port can be changed in the database server installation; 3306 is the default value.
Orchestrator	Any	Oracle Database Server	1521	TCP	Oracle configured Listener	The database port can be changed during Create Listener; 1521 is the default value for the Oracle Listener port. The database instance can be associated with a different listener. Refer to the Oracle configuration.

Ports Used by Web Clients

The following table provides an overview of the ports used for communications from the Web clients.

Communication from Web Clients

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Web Browser (CA EEM Administrator)	Any	CA EEM	5250	TCP	CA EEM configuration	Web Browser accessing the CA EEM UI.
Web Browser (CA Process Automation Web UI user)	Any	Load Balancer	80	TCP	Apache: httpd.conf NGINX: pam-server.conf F5: iRules Config	Load Balancer port for basic communication
Web Browser (CA Process Automation Web UI user)	Any	Load Balancer	443	TCP	Apache: httpd.conf NGINX: secure-pam-server.conf F5: iRules	Load Balancer port for secure communication
Web Services (SOAP) client	Any	Load Balancer	80	TCP	Apache: httpd.conf NGINX: pam-server.conf F5: iRules Config	Load Balancer port for basic communication
Web Services (SOAP) client	Any	Load Balancer	443	TCP	Apache: httpd.conf NGINX: secure-pam-server.conf F5: iRules	Load Balancer port for secure communication
Catalyst REST client	Any	Load Balancer	7000	HTTP	Apache: httpd-proxy.conf NGINX: pam-rest.conf F5: iRules config	CA Process Automation Catalyst container port
Catalyst REST client	Any	Load Balancer	7443	HTTPS	Apache: httpd-proxy.conf NGINX: pam-rest.conf F5: iRules config	CA Process Automation Catalyst container secure port
Web Browser (CA Process Automation Web UI user)	Any	Orchestrator	8080	HTTP	OasisConfig.properties	Browser talks to Orchestrator on this port with basic communication.

From	Port	To	Default Listening Port	Protocol	Configuration	Description
Web Browser (CA Process Automation Web UI user)	Any	Orchestrator	8443	HTTPS	OasisConfig.properties	Browser talks to secure Orchestrators on this port.

Appendix C: 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.

  install_dir/server/c2o/.config/OasisConfig.properties

  install_dir/server/c2o/.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 addresses that change, reconfigure the agent by updating the following file:

  install_dir/PAM Agent/PAMAgent/.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=*xxx.xxx.xxx.xxx*

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 253) 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 252).

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

   See Maintain the DNS Host Name (see page 253).

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 252).
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 151).
   b. Start the Orchestrator (see page 150).

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 D: Troubleshooting

This section describes the troubleshooting methods to use CA Process Automation.

This section contains the following topics:

Unable to Install Agent with Oracle JDK7 Update 51

Previous versions of CA Process Automation use self-signed jars within the Java Web start applications for agent and orchestrator installation. After the availability of JRE7u51/JDK7u51, Oracle escalated the javaws/JNLP security settings.

Symptom:

Due to the default JVM security settings, applets, and web start applications that are self-signed or use self-signed jars fail to start.

Solution:

To address the issue, CA Process Automation 04.2.01 Orchestrator and Agent components now only use CA-signed jars.

Note: If an agent uses JDK6, disable FIPS 140 compliance on all orchestrators (including each node of a clustered orchestrator). To disable FIPS 140 compliance on all orchestrators, set the *pam.fips.mode.enabled* parameter to “false” in the OasisConfig.properties file and restart the orchestrator.

Connector Installation Changes for Oracle JDK7u51 Support

If you use Oracle JDK7u51 and above on the CA Process Automation orchestrator, consider the following points:

- Upgrading to CA Process Automation 04.2.01

  When you upgrade CA Process Automation r4.x to CA Process Automation 04.2.01, install the 4.2.1 Classic Connectors to upgrade the existing classic connectors.

- Installing CA Process Automation 04.2.01

  For a new CA Process Automation 04.2.01 installation, install the CA Process Automation 04.2.01 Classic Connectors.

  Note: For more information on classic connectors, see the CA Process Automation Connector Readmes in the *Connector Installation Media*.

CPU Usage Spikes in server nodes with Secured Simplified Communication and Load Balancer

Symptom:

When a clustered Orchestrator is configured to use secure (HTTPS) communication and agents are configured to use simplified communication with an NGINX load balancer, CPU usage spikes can occur in server nodes when the orchestrator is restarted while multiple agents are active.

Solution:

Note: This is not a recommended approach. Use the following approach only for the above problem.

To fix the problem, configure the clustered Orchestrator to use non-secure (HTTP) communication between load balancer and orchestrator as follows:

1. Add the following properties in the OasisConfig.properties file for all orchestrator nodes:
   - pam.transport.unsecured.connector.flag: Set the value to true.
   - pam.transport.unsecured.connector.port: Specify an integer value. Default value is 80.
2. Edit the following entries in the secure-pam-server.conf file to enable non-secure websocket connection between Load Balancer and nodes:
   - // websocket connections

     upstream node1{

     server <hostname of machine where you have installed node1>: Specify the same port number as pam.transport.unsecured.connector.port

     }

     Note: Specify the same port number as pam.transport.unsecured.connector.port for upstream node2.
   - Change https to http in the following entries:

     location = /ws/node1 {

     proxy_pass http://node1; }

     location /ws/node1/ {

     proxy_pass http://node1;}

     location = /ws/node2 {

     proxy_pass http://node2; }

     where node2 is the upstream name

     location /ws/node2/ {

proxy_pass http://node2; }

3. Restart Orchestrator nodes and Load Balancer.

CPU Usage Spikes in server nodes with Secured Simplified Communication and F5 Load Balancer

Symptom:

When a clustered Orchestrator is configured to use secure (HTTPS) communication and agents are configured to use simplified communication with an F5 load balancer, CPU usage spikes can occur in server nodes when the orchestrator is restarted while multiple agents are active.

Solution:

Note: This is not a recommended approach. Use the following approach only for the above problem.

To fix the problem, configure the clustered Orchestrator to use non-secure (HTTP) communication between load balancer and orchestrator as follows:

1. Add the following properties in the OasisConfig.properties file for all orchestrator nodes:
   - pam.transport.unsecured.connector.flag: Set the value to true.
   - pam.transport.unsecured.connector.port: Specify an integer value. Default value is 80.
2. Add the following pools for each CA Process Automation cluster and use the non-secure server port (by default, 80) and http protocol for each member:
   - NODE_1 with the member PAM Domain node1
   - NODE_2 with the member PAM Domain node2

   Note: For more information on how to create two F5 pools for each CA Process Automation cluster, see the Create Two F5 Pools for Each CA Process Automation Cluster in the *CA Process Automation Installation Guide*.
3. Modify the iRule Definition as follows:
   - Add the entries NODE_1 and NODE_2 to the following lines:
     - set NODE1 "NODE_1"
     - set NODE2 "NODE_2"
   - Remove the line:
     ```
     set WSPORT "443"
     ```
   - Modify the URL mapping for the following URLs as follows:
     ```
     "/ws/node1" { SSL::disable serverside
                                    pool $NODE1
     }
     "/ws/node1*" {  SSL::disable serverside
                                     pool $NODE1
     }
     ```

```
"/ws/node2" { SSL::disable serverside
                                    pool $NODE2
}
"/ws/node2*" {  SSL::disable serverside
                                    pool $NODE2
}
```

4. Restart Orchestrator nodes and Load Balancer.

Simplified Communication Fails After Changing the Orchestrator URL

You can change the URL of the Domain Orchestrator during a reinstall or you can make a port change to the existing URL through an OasisConfig.properties file change.

Symptom:

Agents that use simplified communication stop communicating with an Orchestrator after that Orchestrator URL is changed, including a change in port number.

> **Note:** Simplified communication is configured by clearing the “Use deprecated communication” check box in the agent properties.

Solution:

Reinstall all agents that are associated with touchpoints in the environment with the affected Orchestrator.

Oracle Locks Can Occur If You Do Not Shut Down Running Processes Before Starting an Upgrade

For a smooth upgrade to Release 4.2, verify that there are no running instances before starting the upgrade.

Symptom:

If you start an upgrade where processes are running and the Runtime database is on an Oracle database server, you can experience issues with a lock not being released. After the upgrade, when the server tries to adjust the database, an exception similar to the following can occur:

ORA-01591 lock held by in-doubt distributed transaction

This causes the environment to fail functionally after the upgrade.

Note: This situation rarely occurs.

Solution:

Resolve transactions noted by "ORA-01591 lock held by in-doubt distributed transaction" in the following cases:

- The in-doubt transaction has locks on critical data or undo segments.
- The cause of the machine, network or software failure cannot be repaired quickly.

To correct this problem, manually execute the ROLLBACK on the Oracle database.

Follow these steps:

1. Identify the transaction identification number for the in-doubt transaction by querying DBA_2PC_PENDING views. Execute following query for the same:

   ```
   select * from DBA_2PC_PENDING
   ```

2. Check the state of the transaction. If state is PREPARED then either:
   - Force a commit using the COMMIT FORCE statement
   - Force a rollback using the ROLLBACK FORCE statement.

     ROLLBACK FORCE '*your local transactionID on this node*'

     For example:

     ```
     ROLLBACK FORCE '1.13.5197';
     ```

Third_Party_Installer_unix.sh: Permission Denied

Symptom:

If you execute the Domain installer, the following error message is displayed:

Third_Party_Installer_unix.sh: Permission denied.

Solution:

In Red Hat Enterprise Linux, to execute permissions on the .sh file, enable the execute permissions on the .sh files. For example, execute permission on the .sh files using the following commands:

```
chmod a+x Domain_Installer_unix.sh
chmod a+x Third_Party_Installer_unix.sh
```

Stop Processes Before an Upgrade

If you are upgrading from a previous CA Process Automation release, do not have any in-flight processes during the upgrade (waiting, running, blocked, and so on). Even though CA Process Automation has a mechanism to recover from failures in such cases, all the in-flight processes may not be recovered.

See "Carry Out Upgrade Prerequisites" in the Upgrade to the Current Release chapter in the *Installation Guide* for this prerequisite and other prerequisites to upgrading.

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.

Potential Problem When Running CA Process Automation on a VMWare Server When Using the E1000 Network Interface

Symptom:

The root causes of this problem are rare, sporadic, socket I/O failures, which may leave the calling software waiting indefinitely for a read to complete.

From the users perspective the most typical symptom will be the unexpected hanging of processes that normally complete without issue, which resume and complete as expected following a restart of the CA Process Automation Orchestrator. This can impact a small subset of processes, or all running processes. It has no correlation with Orchestrator uptime, and may manifest shortly after a restart, or, after days, weeks, or months of otherwise flawless Orchestrator functionality.

This problem has only been seen in environments running high volumes of CA Process Automation processes. In most environments where the E1000 NIC is installed the problem has never occurred, or occurred so infrequently that it has not been detected.

Solution:

This problem is very difficult to confirm. If this problem occurs, often the CA Process Automation thread is stuck on a socket read, and no relevant errors are written to the log files, and confirmation of the problem requires reviewing a series of Java thread dumps taken during an occurrence of this problem to confirm the operator is stuck on a socket read.

When errors are observed in relation to this problem, they tend to indicate generic connection errors which could have other legitimate and unrelated causes. The following is such an example:

```
2013-07-24 18:55:23,219 WARN  [org.hibernate.jdbc.AbstractBatcher]
[nPool Worker-23] exception clearing maxRows/queryTimeout
com.microsoft.sqlserver.jdbc.SQLServerException: The connection is
closed.
                at
com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverErro
r(Unknown Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerConnection.checkClosed(Unkno
wn Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.checkClosed(Unknow
n Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.getMaxRows(Unknown
Source)
                at
org.jboss.resource.adapter.jdbc.CachedPreparedStatement.getMaxRows
(CachedPreparedStatement.java:367)
```

```
                at
org.jboss.resource.adapter.jdbc.WrappedStatement.getMaxRows(Wrappe
dStatement.java:378)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:272)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:209)
```

. . . and so on.

In these cases identification of the problem is tentative, and other causes for communication failure must be excluded.

Frequent process failure, or a repeatable failure of an individual operator or operators likely indicate other unrelated problems within the process design or Orchestrator functionality.

At sites where this problem has been confirmed, reconfiguring the VMWare server from an E1000 Network Interface Card driver to a VMXnet-3 NIC driver is seen to be a very effective mitigation.

CA Technologies is hesitant to declare this a complete resolution as the incident rate for this is very rare and timeframe between occurrences even with the E1000 NIC can be quite long.

If verification of the issue is required prior to making this change, please contact Support for assistance setting up the logging and Java thread dumps required to troubleshoot and verify this particular issue.

Oracle Bug # 9347941

Important! When running with versions of the Oracle RDBMS prior to release 11.1.0.7 CA Process Automation would occasionally hit known Oracle RDBMS defect 9347941 in which concurrent inserts of CLOB data where the individual column values exceed 52K bytes in size have such columns updated incorrectly with data past the 52K offset replaced by spaces. This issue has been seen using both 10g and earlier 11g versions of the Oracle RDBMS.

Symptom:

CA Process Automation process would become stuck. You need to reset the process at the corresponding operator where the process is stuck to continue the process execution to complete. This problem is infrequent and occurs only with extremely high rates of update contention.

Solution:

This has not been seen when running either version 11.1.0.7 or 11.2.0.2 of Oracle, and It is recommended that sites using Oracle for their CA Process Automation databases be running version 11.1.0.7 or 11.2.0.2 or later.

Limitations in Internet Explorer

Internet Explorer limits the agent installation in a network other than the network where Domain Orchestrator is installed.

Symptom:

Access the Domain Orchestrator using Internet Explorer and install the CA Process Automation Agent in a network other than the network where Domain Orchestrator is installed. The installation may fail while downloading JAR files for installation.

Solution:

A possible cause of this sporadic issue might be that Java is unable to load JAR files while routing through the proxy in Internet Explorer. To mitigate this issue, change Java Network Settings to the Direct Connect option before you install the Agent.

Follow these steps:

1. Open the Java Control Panel on the host system where you install the Agent.
2. Open Network Settings from the General tab.

   The Network Settings page appears.
3. Select the Direct Connect option and click OK to save changes.
4. Install the Agent.

CA Process Automation Installation on Dual Stack (IPv4 and IPv6) Network Environments

If you install CA Process Automation on dual stack (IPv4 and IPv6) network environments, CA Process Automation may fail to boot up.

Symptom:

When you install CA Process Automation on dual stack (IPv6 and IPv4) network environments, you may experience issues while bringing up or accessing the following CA Process Automation components across network:

- Domain Orchestrators
- Orchestrators
- Agents

Solution:

Disable IPv6 stack on the host system where any of the following CA Process Automation components are running and restart the services:

- Domain Orchestrators
- Orchestrators
- Agents

Slow Performance Using MySQL

Symptom:

When I install CA Process Automation using MySQL or Oracle as the database, I notice performance is lacking.

Solution:

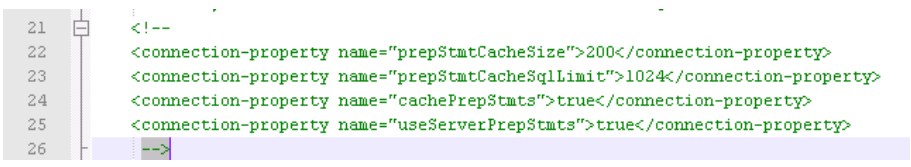
Post-installation, modify the oasis-ds.xml file to enhance CA Process Automation performance.

Follow these steps:

1. Locate and open the oasis-ds.xml file, located in:

   install_dir/server/c2o/ext-deploy

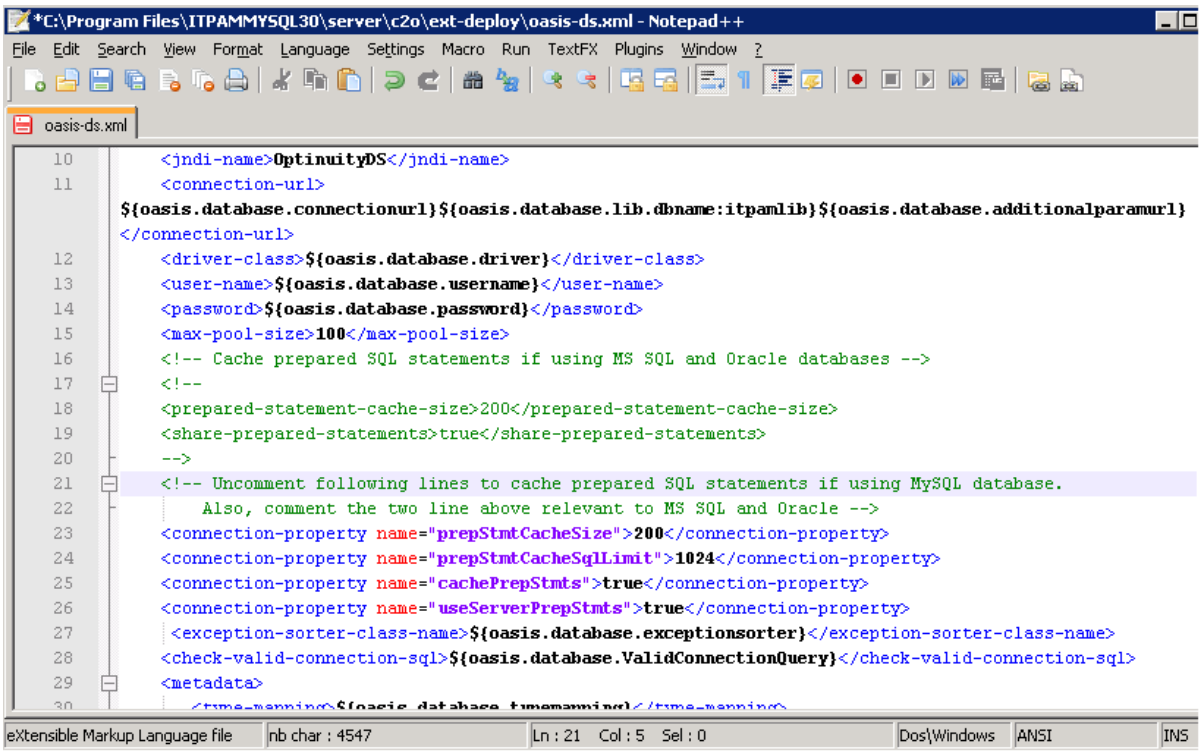
2. Uncomment the following lines:



3. Comment the following lines:

```
16      <!-- Cache prepared SQL statements if using MS SQL and Oracle databases -->
17      <prepared-statement-cache-size>200</prepared-statement-cache-size>
18      <share-prepared-statements>true</share-prepared-statements>
```

The updated file should look like this:



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 Version 4.0 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'
```

Note: For an alternative solution that retains the Orchestrator ID, see TEC596124

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 E: Upgrade Examples

This section contains the following topics:

Example: Upgrade Any Node of the Domain Orchestrator from 3.1 SP01 to Release 4.2 on Windows

The following example is the first of two related examples on upgrading a clustered Domain Orchestrator from 3.1 SP01 to Release 4.2 on a Windows operating system. The examples include selected screenshots and commentary for the following scenario:

- Domain Orchestrator node 1 - pam-sandbox-n1
- Domain Orchestrator node 2 - pam-sandbox-n2
- Load Balancer for Domain Orchestrator - pam-sandbox-LB

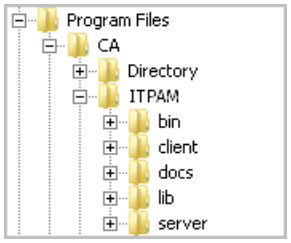
These are the steps:

1. Log in to the host with the node of the clustered Domain Orchestrator that you plan to upgrade.
2. Open the CA Process Automation release you are upgrading. For example, from the Start menu, select Programs, CA, CA Process Automation Domain 3.1 SP01, Start CA Process Automation Management Console.

   Note: This is an easy way to verify that CA EEM is running and that your database server is active. This is a prerequisite to upgrade.

3. Click Sign Out, close the CA Process Automation Management Console, and stop the Orchestrator Service. (If you open Services, you can verify that the service is not in Started status. Do not proceed while the Status is "Stopping." Refresh this view and wait until the Status field is cleared.

4. Navigate to the DVD1 folder on the installation media and start the Domain_Installer_windows.bat.
5. Click Next to move through the initial pages of the Third-Party Installer Setup wizard:
   - Welcome to the CA Process Automation 3rd Party Installer Setup Wizard
   - License agreement - I accept the terms of the License Agreement
6. For Select Destination Directory, browse to the exact directory that contains the files for CA Process Automation 3.1sp01: bin, client, docs, lib, and server. This directory is typically ITPAM, but it could have a name you previously provided.

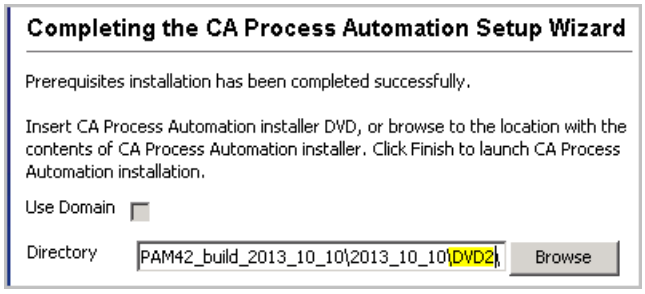


Important! You must point to the correct directory so that the installation process recognizes your previous configuration options.

7. Click Next to proceed through Prerequisites for CA Process Automation Installation.

   Installation of third-party components begins.
8. When the JDBC Jars for Installation page appears, click Add Files if you are using a MySQL database server or a SQL Server. Browse to the location of the appropriate jar file.

   For example, the JDBC driver for SQL Server has changed, browse to DVD1\drivers\jtds-1.3.jar for SQL Server.
9. When the Completing the CA Process Automation Setup Wizard page appears,
   a. Change the last directory of the displayed path from DVD1 to DVD2.



   b. Click Finish.

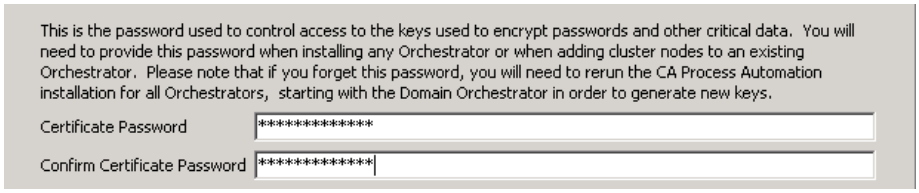
      The following message appears: "Copying CA Process Automation installer. This may take a few minutes to complete, please wait."

10. When the Welcome to CA Process Automation Domain Setup Wizard appears, click through the initial pages of the wizard:
    - Language
    - Welcome to the CA Process Automation Domain Setup Wizard
    - License Agreement- I accept the terms of the License Agreement.
    - Java Home Directory - this is picked up automatically, for example, C:\Program Files\Java\jdk1.7.0_x.
    - Reinstall/Configure - the Reinstall option means **Upgrade**.

      The copying configuration message appears.
    - Configuration Screen

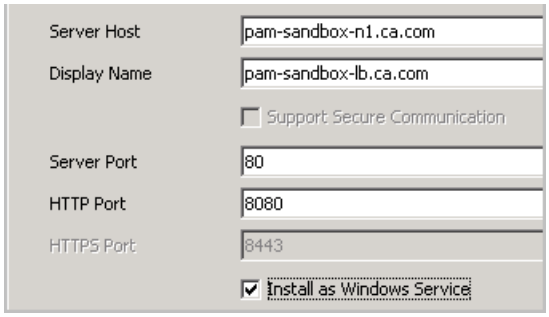
      The following example includes our sample data:

11. When the Set Certificate Password appears, enter the *same* certificate password that was used in the previous release, and then click Next.

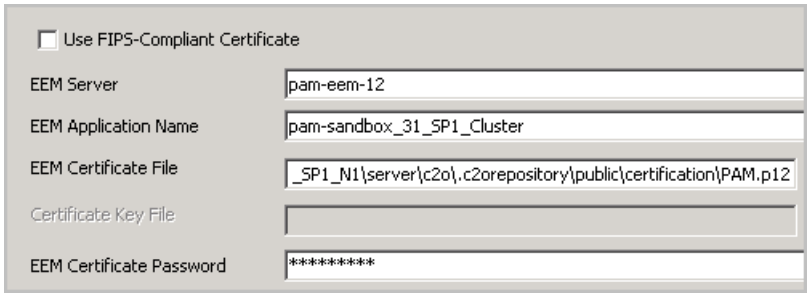


12. Click Next to Select Start Menu Folder - the default is CA Process Automation 4.2
13. For General Properties, click Next. Install as Windows Service is selected by default.

    The following example includes our sample data:

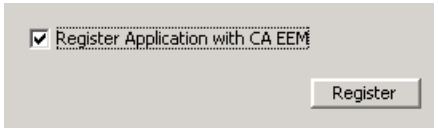


14. Click Next to proceed through the following pages:
    - Scripts Temporary Directory
    - Powershell Execution Policy
15. When the Embedded Entitlements Manager (EEM) Security Settings appears, entries from your previous configuration are populated by default. For example:

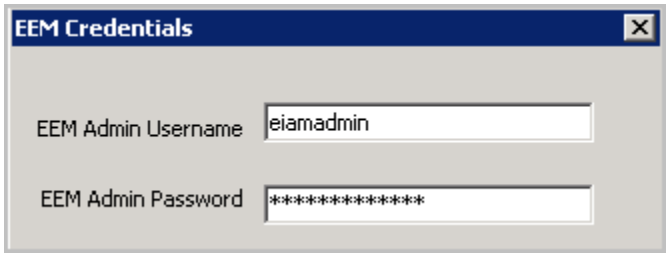


    a. Skip the Default Active Directory Domain field unless you configured CA EEM to use multiple Microsoft Active Directories. In this case, enter the name of one of the ADs you configured.

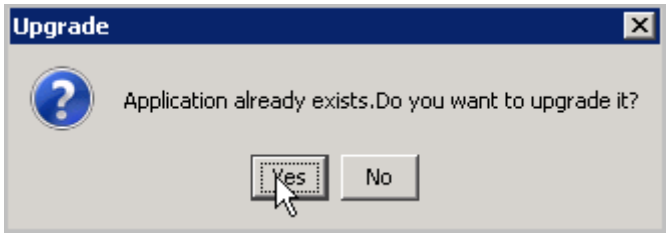
    b. Select Register Application with CA EEM and click Register.



    c. Supply credentials for logging into CA EEM as the EiamAdmin administrator and click OK.



    d. Click Yes to agree to upgrade.

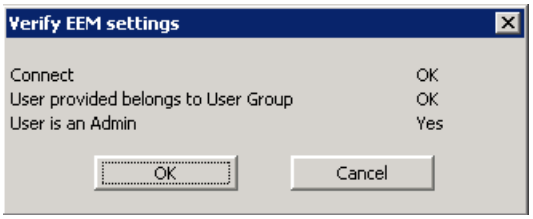


e. Click OK to the "Application Upgraded" message.

f. (Optional). Click Test EEM Settings and complete the Verify EEM settings:

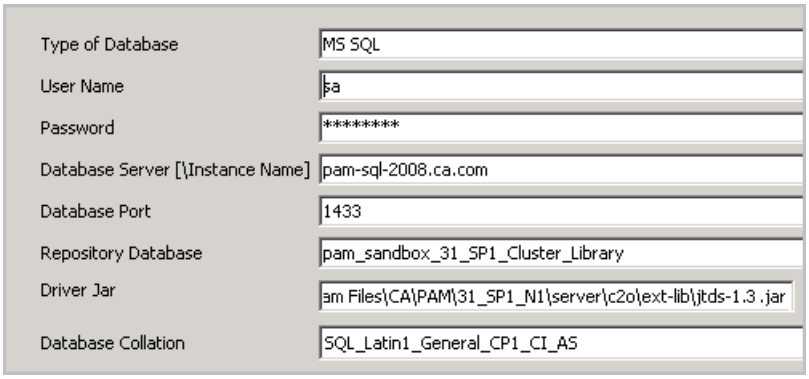
- If your user credentials are stored in CA EEM, enter the user name and password for your CA Process Automation user account.
- If CA EEM uses Active Directory, entered your AD credentials.

Respond to the confirmation message.



16. As the following Database Settings appear, click Test Database Settings to verify that "Test is successful" is displayed. Click Next.
    - Repository database (also known as the Library database)
    - Runtime database
    - Reporting database

    The following example includes our sample data:



17. For Additional Jars for Installation, click Next or select from the displayed list and add additional files if required.
18. Wait while Setup upgrades (installs) the CA Process Automation Domain.
19. When the Completing the CA Process Automation Domain Setup Wizard appears, click Finish.
20. Log off the server on which node 1 of the clustered Domain Orchestrator was upgraded.

Note: If you have connectors to update, defer starting the Orchestrator service until this update is complete.

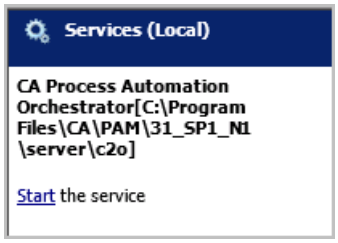
Example: Upgrade Another Node of the Domain Orchestrator from 3.1 SP01 to Release 4.2 on Windows

The following example is the second of two related examples on upgrading a clustered Domain Orchestrator from 3.1 SP01 to Release 4.2 on a Windows operating system. The examples include selected screenshots and commentary for the following scenario:

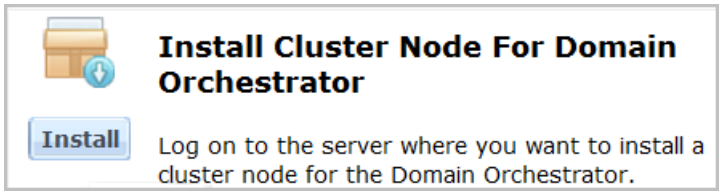
- Domain Orchestrator node 1 - pam-sandbox-n1
- Domain Orchestrator node 2 - pam-sandbox-n2
- Load Balancer for Domain Orchestrator - pam-sandbox-LB

These are the steps:

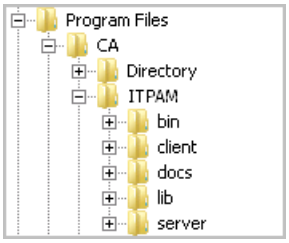
1. Log on to the first server you upgraded. Start the Orchestrator Service through Administrative Tools, Services. Notice that the path is the same path in which you initially installed CA Process Automation.



2. Log onto the server on which another node (for example, node2) of the clustered Domain Orchestrator is installed.
3. Browse to the Domain URL, the load balancer for the Domain Orchestrator. In this example, it is http://pam-sandbox-lb/itpam.
4. Log in, click the Configuration tab, and then click the Installation palette (bottom left).
5. Under Install Cluster Node For Domain Orchestrator, click Install to begin the upgrade.



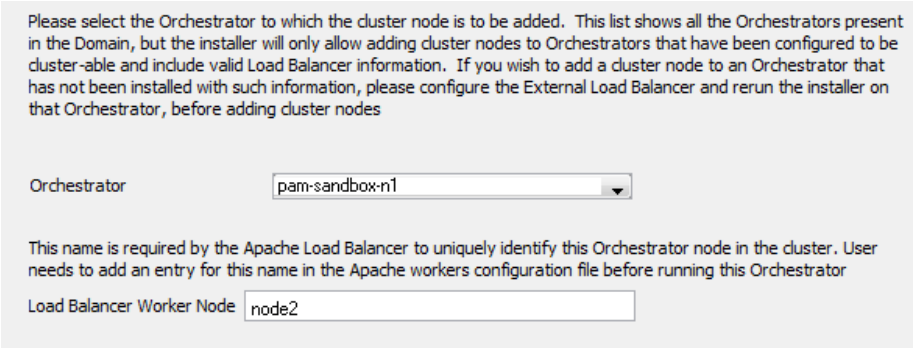
6. The language selection dialog appears first. Click OK.
7. Click through the following Wizard pages:
   - Welcome to the CA Process Automation 3rd Party Installer Setup Wizard.
   - License Agreement - select I accept the terms of the license Agreement
8. For Select Destination Directory, browse to the exact directory that contains the files for CA Process Automation 3.1sp01: bin, client, docs, lib, and server. This directory could have the default name or a name you previously provided.



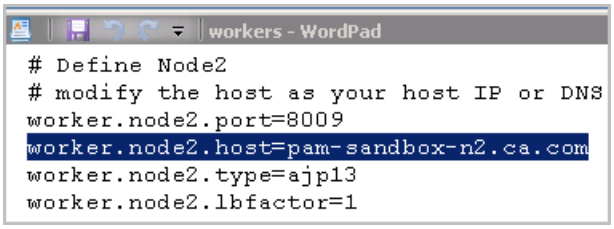
Important! You must point to the correct directory so that the installation process recognizes your previous configuration options.

9. Click through the following Wizard pages:
   - Prerequisites for A Process Automation installation - invokes installation.
   - Completing the CA Process Automation Setup Wizard with Use Domain selected - Click Finish

     Wait until the next page appears. There is no visual indicator of the processing that precedes the display of the next page.
   - Welcome to the CA Process Automation Domain Setup Wizard
   - License Agreement
10. If you upgraded your JDK, browse to the Java Home Directory, for example, C:\Program Files\Java\jdk1.7.0_45
11. When the Configuration Screen appears,
    a. Click the Orchestrator drop-down list and select the node of the Domain Orchestrator that you upgraded first.

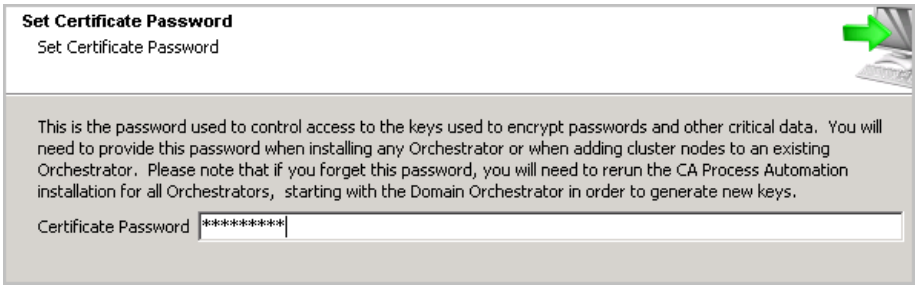


b. Enter a value in the Load Balancer Worker Node field. Type the designator for the node (node2, node3, node4) on which you are doing the upgrade. Consider the format worker.**node2**.host=*current-host*, as it was defined in workers.properties in the *apache_install_dir/conf* folder.



In this example, node2 of the Domain Orchestrator cluster is defined as the value for worker.**node2**.host=pam-sandbox-n2 in workers.properties. The load balancer FQDN is prepopulated in the Public Host Name field.

12. Type your company name.
13. Type the *same* certificate password that you entered when you installed the previous node of the Domain Orchestrator. This is the *same* certificate password that was used by the Domain Orchestrator in the previous release.



14. Click through the following pages, which use settings from node1 in this example.
    - Select Start Menu Folder.
    - General Properties page (Install as Windows Service is not shown but is assumed).
    - Scripts Temporary Directory
    - PowerShell
    - CA Embedded Entitlements Manager CA EEM Security Settings
    - Database Settings - Repository
    - Database Settings - Runtime
    - Database Settings - Reporting

    The upgrade installation begins.
15. When Completing the CA Process Automation Domain Setup Wizard page appears, click Finish.

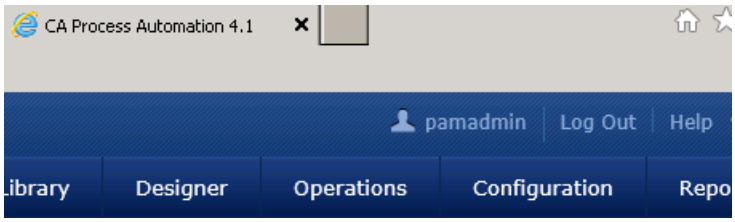
Example: Upgrade a Non-clustered Orchestrator from 4.1 SP01 to Release 4.2 on Windows

The following example provides selected screenshots that resemble what you see when you upgrade a non-clustered Orchestrator from 4.1 SP01 to Release 4.2 on a Windows operating system. If you are not familiar with the CA Process Automation installation wizard, you may find this useful.

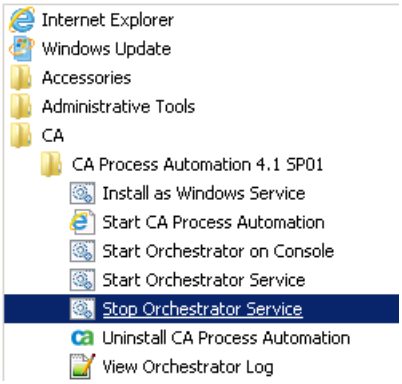
These are the steps:

1. Log in to the host on which the Domain Orchestrator is installed.
2. Open the CA Process Automation release you are upgrading. For example, from the Start menu, CA, CA Process Automation 4.1 SP01, Start CA Process Automation.

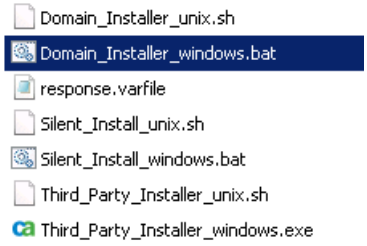
   Note: This is an easy way to verify that CA EEM is running and that your database server is active. This is a prerequisite to upgrade.



3. Log out of CA Process Automation, close the browser, and stop the Orchestrator Service.For example, from the Start menu, select CA, CA Process Automation 4.1 SP01, Stop Orchestrator Service. (If you open Services, you can verify that the service is not in Started status.)



4. Navigate to the DVD1 folder on the installation media and start the Domain_Installer_windows.bat.



5. Click Next to move through the initial pages of the wizard:
   - Language
   - Welcome to the CA Process Automation 3rd Party Installer Setup Wizard
   - License agreement - I accept the terms of the License Agreement
6. On the Select Destination Directory page, verify that this directory is set to the same directory as the release that you are upgrading from. In this example, the default directory for both 4.1 SP01 and 4.2 is the same:

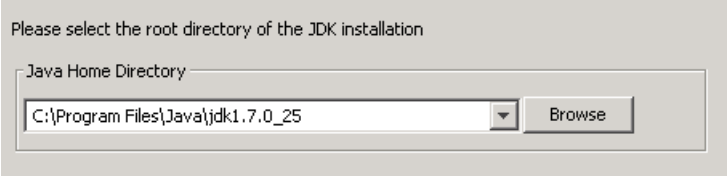
   `C:\program files\ca\pam`

   Note: If you installed the previous release in a folder other than the default, navigate to that folder.
7. Click Next to move through the initial pages of the wizard:
   - Prerequisites for CA Process Automation Installation

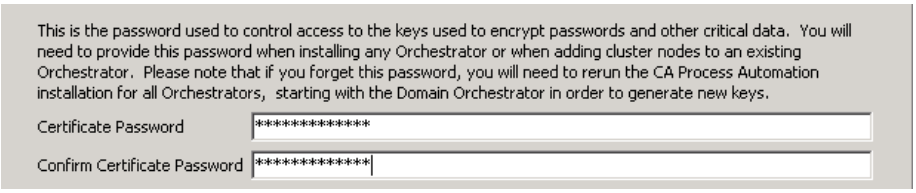
     Installation begins, including installing Active MQ and installing third party components.
   - JDBC Jars Installation (The default is to use the JDBC jars specified during the Domain Orchestrator upgrade.)
   - Prerequisites for CA Process Automation installation (successfully done)
8. When the Completing the CA Process Automation Setup Wizard appears, replace DVD1 with DVD2 in the Directory path. Then click Finish.

   The message appears: "Copying CA Process Automation installer. This may take a few minutes to complete, please wait." You may experience a time lag between the close of this page and the opening of the Welcome page.
9. When the Welcome to CA Process Automation Domain Setup Wizard appears, click through the initial pages of the wizard:
   - Language
   - Welcome to the CA Process Automation Domain Setup Wizard
   - License Agreement- I accept the terms of the License Agreement

10. For CA Process Automation Domain, Please set Java Home Directory, browse to the correct directory.



11. Continue, clicking through pages:
    - CA Process Automation Domain, Reinstall/Configure - Reinstall is the only option available for an upgrade.
    - CA Process Automation Domain, Configuration Screen
12. When the Set Certificate Password appears, enter the *same* certificate password that the Domain Orchestrator uses. This certificate password must match the one entered when this non-clustered Orchestrator was initially installed. Click Next



13. Click through the Select Start Menu Folder to use your previous selection.
14. On the General Properties page, note the following changes in defaults for the Orchestrator server port:

    Server Port

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

    Default: 80 (basic: HTTP), or 443 (secured: HTTPS)

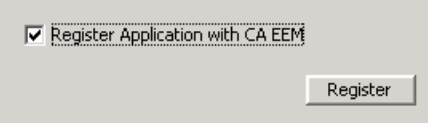
    Deprecated Server Port

    (Upgrade/re-install only) The Server Port value that was defined for a previous release of CA Process Automation.

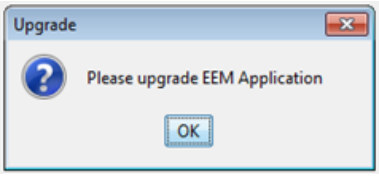
    Default: 7001
15. Click through the following pages, making changes at your discretion.
    - Scripts Temporary Directory
    - Powershell Execution Policy

16. When the Embedded Entitlements Manager (EEM) Security Settings appears,

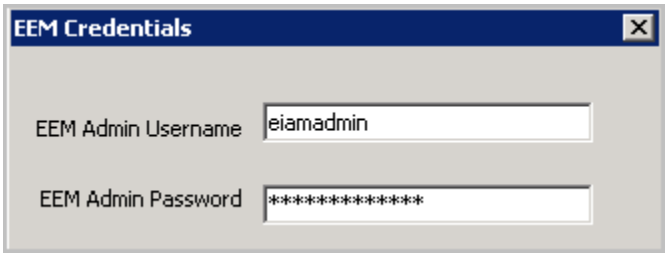
    a. Select Register Application with CA EEM and click Register. This is always a good idea to do for an upgrade because a new release can contain changes or additions to CA EEM policies for CA Process Automation. When no changes are made between releases, you will see a message that no upgrade is required.



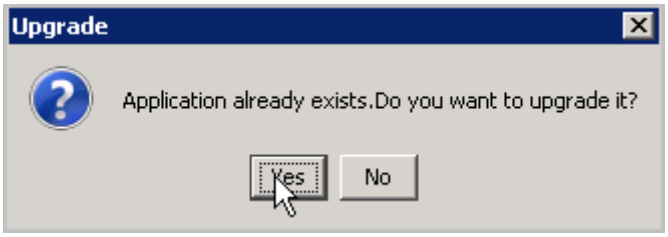
    b. If you attempt to exit this page without registration and the installation process detects a CA Process Automation version upgrade, the installation process prompts you to select Register Application with CA EEM and then click Register.



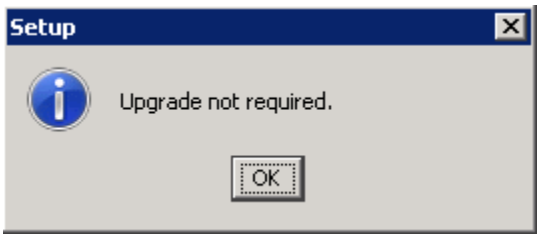
    c. Supply credentials for logging into CA EEM as the EiamAdmin administrator.



    d. Agree to upgrade. The installation process detects the CA EEM server version and choses the appropriate SDK.



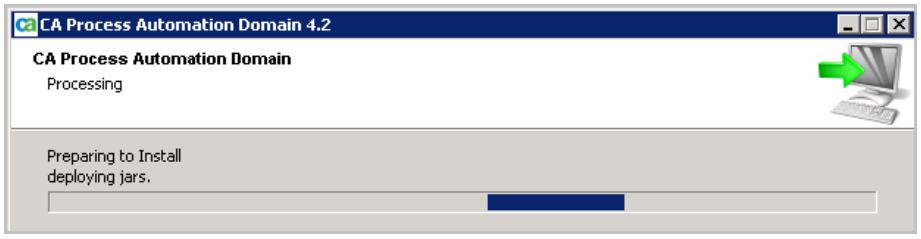
    e. If upgrade is not required, this message appears:



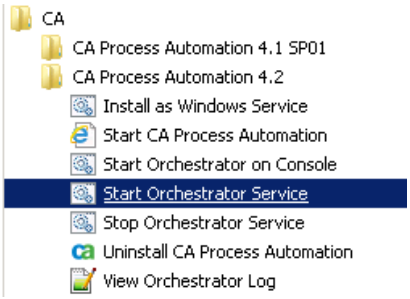
    f. Click OK when the Application Registered confirmation appears.

17. Click through the Database Settings since you have already defined these:
    - Repository database
    - Runtime database
    - Reporting database
18. Click through Additional JARs for installation if there is nothing to add.

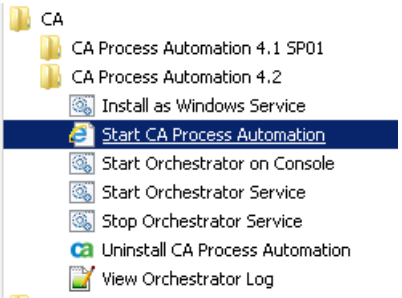
    Setup upgrades (installs) the CA Process Automation Domain.



19. When the Completing the CA Process Automation Domain Setup Wizard appears, click Finish. Allow time for the schema updates to complete before attempting to start CA Process Automation.
20. Start the Orchestrator Service.



21. Start CA Process Automation.



Upgrading from a Release Prior to Release 3.1 SP01

You cannot directly upgrade from CA IT Process Automation Manager (CA IT PAM) Release 2.x, Version 3.0, or 3.0 SP01 to CA Process Automation Release 4.2. You must first perform an intermittent upgrade.

Follow these steps:

1. Prepare for the upgrade.

   Upgrading from CA IT Process Automation Manager Release 3.0 SP1 requires twice the available disk space than the existing CA IT PAM databases require. To provide adequate space to your Database Server and to speed the upgrade process, the best practice is to purge unnecessary archive records before upgrading.

2. Upgrade from any of the previous releases to CA Process Automation 3.1 SP01.

   - CA IT PAM Release 2.x
   - CA IT PAM Version 3
   - CA IT PAM Service Pack 3.0 SP01

   Note: For information about this interim upgrade, download the appropriate Installation Guide from Customer Support.

3. Upgrade from CA Process Automation Service Pack 3.1 SP01 to CA Process Automation Release 4.2 as described in How to Upgrade CA Process Automation.

Index