CA Server Automation

Installation Guide

Release 12.8.1

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.

CA Technologies Product References

This document may reference the following CA Technologies products and components or third-party components:

- CA Configuration Automation, formerly CA Application Configuration Manager (CA ACM)
- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager (CA ITAM)
- CA IT Client Manager (CA ITCM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Process Automation, formerly CA IT Process Automation Manager (CA IT PAM)
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Software Delivery, a component of CA IT Client Manager
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA SystemEDGE

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This guide describes the steps to install the CA Server Automation software.

Related Publications

The CA Bookshelf provides the following CA Server Automation publications:

Administration Guide

Describes product architecture, troubleshooting, concepts, and configuration tasks for administrators.

Installation Guide

Describes installation prerequisites, best practices, and procedures for CA Server Automation.

Reference Guide

Provides detailed information about AutoShell, CLI scripting commands, and log files.

Performance Metrics Reference

Describes the performance metrics that are available for monitoring the systems performance of the supported platforms.

CA Process Automation Connector Reference Guide

Provides detailed information about CA Process Automation connectors and use cases.

Online Help

Provides information to help you complete tasks using the CA Server Automation user interface.

Reservation Manager Help

Provides information to help users and administrators complete tasks using the Reservation Manager user interface.

Release Notes

Provides information about new and changed features and product implementation information including operating system support, system requirements, and how to contact Technical Support.

Service Response Monitoring User Guide

Provides installation and configuration details of SRM.

SystemEDGE User Guide

Provides end-user information about the SystemEDGE agent.

SystemEDGE Release Notes

Provides information about new and changed features and agent implementation information including operating system support, system requirements, and how to contact Technical Support.

To view PDF guides, download and install Adobe Reader from the Adobe website if it is not already installed on your computer.

Chapter 2: Plan Your Installation

This section contains the following topics:

Plan the Installation

You can install the product software using one of the following ways:

Installation Wizard

Installs and upgrades CA Server Automation basic components and SystemEDGE.

You can run the installation wizard after initial installation to install new components. You cannot use the installation wizard to reinstall, repair, or reconfigure existing components.

To install and upgrade SystemEDGE, see the *SystemEDGE User Guide*.

Command line

Requires you to create property files (silent installation).

Review the following information to prepare for installation:

- *Release Notes* for system requirements
- *Administration Guide* for configuration and management
- Other CA integration product documentation

Prepare Servers

The servers that you select to host the CA Server Automation software must meet the system requirements specified in the *Release Notes*.

CA Server Automation Server

The wizard provides a centralized installation, with components installed on a single Windows server. If your site requires it, you can install some components (for example, AIMs and Autoshell) across multiple servers. However, the CA Server Automation components (core) are *not* distributable.

To distribute components across more than one server, verify the following conditions:

- Open the communication ports if components are installed across firewalls.
- Install the Microsoft SQL Management Tools (OSQL, BCP) on the Microsoft SQL server database (Management Database).
- Use the same authentication (Windows or SQL) for the Management Database and the Performance Database.
- Synchronize all server clocks.

Use the following table to prepare the server for installing CA Server Automation.

Server	Requirements
For installing CA Server Automation	■ Valid path for installing CA Server Automation is identified. ■ Microsoft SQL Server is accessible and configured. ■ CA EEM server (local or remote) and users are identified. ■ Active Directory is configured (if applicable). ■ Required network ports are identified and open. ■ Additional runtime locales are identified (if applicable). ■ Community strings are defined. ■ DNS server is working properly. ■ If you are using DHCP for the IP address assignment, DHCP is configured to update the DNS server dynamically. ■ Java Quick Test Pro (QTP) plug-in is not installed. ■ Antivirus programs are stopped before installation. ■ All systems and databases are backed up.

Management Database Requirements

Use the following table to prepare the Management Database servers for installation.

Server	Other Requirements
Management Database Server	■ TCP/IP is enabled. ■ Remote connections are enabled. ■ Authentication mode is enabled (mixed mode or Windows mode). ■ TCP/IP port for the instance is static (dynamic is not supported). ■ No existing databases are named AOM2 or DPM. ■ No IP address is used as the server name for the local database.
Clients	■ The system PATH must have an entry for the client (or CA Server Automation does not recognize that the SQL Server is installed). ■ OSQL.EXE and SQLCMD.EXE are in *one* of the system PATH entries.

Database Sizes for Best Performance

During installation, select an initial size for the Management Database. Selecting an appropriate initial size can avoid incremental resizing that leads to data fragmentation and performance issues.

Review the following table to select the best initial size for the Management Database.

Initial Size	Number of Systems	Disk Space
Small	1,000	1 GB—core components 500 MB—log files
Medium	5,000	5 GB—core components 1 GB—log files
Large	10,000	10 GB—core components 5 GB—log files

Note: The SQL Server databases are set to Full Recovery Model by default, so the transaction log grows until it is backed up. Regularly schedule database backups.

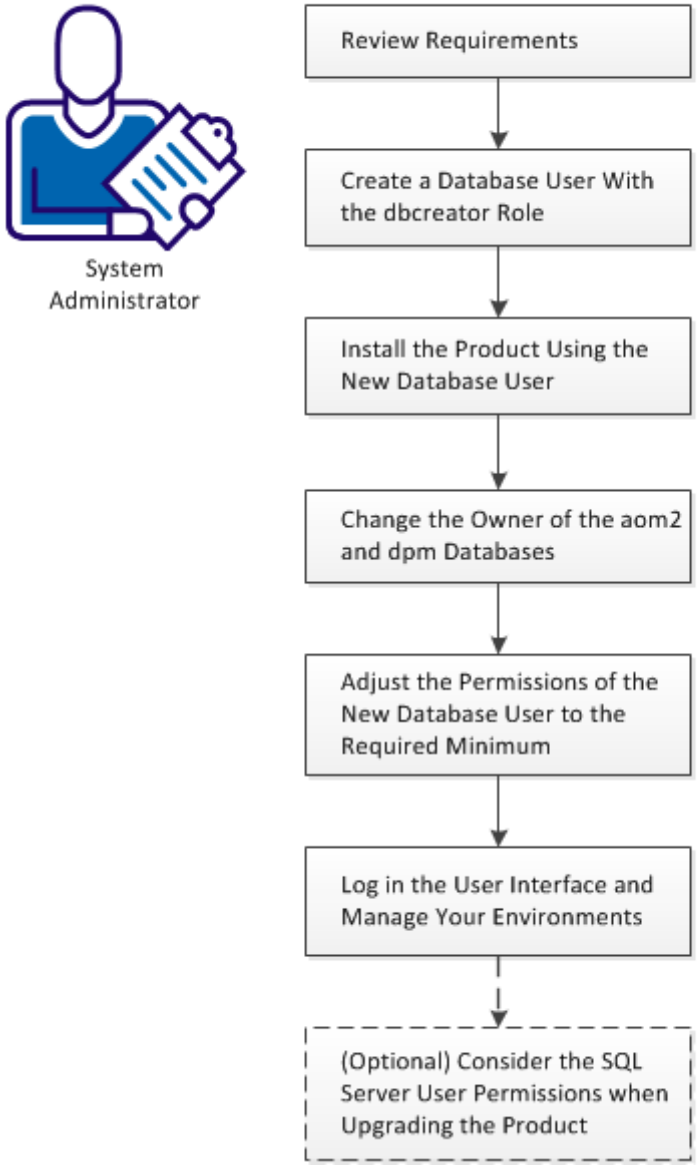
Note: The Performance database defaults to 500 MB and increases automatically as needed.

How to Adjust SQL Server User Permissions to the Required Minimum

As a System Administrator you want to minimize the permissions required by CA Server Automation to access its SQL Server databases.

The following diagram illustrates the required steps to adjust the permissions.

How to Adjust SQL Server User Permissions to the Required Minimum



Follow these steps:

Review Requirements

Review the following requirements before you start changing user permissions of the CA Server Automation database user:

- You are familiar with the administration of Windows Server and SQL Server.
- The system on which you want to install CA Server Automation meets the requirements that are specified in the Release Notes.
- SQL Server is installed according to the requirements specified in the Installation Guide and Release Notes.
- You can use SQL Server Authentication or Windows Authentication.
- You can use one of the following account types to install CA Server Automation:
  - The domain user (domain\domainuser)
  - The local user (system\localuser)
  - The local administrator (system\administrator)

  The account that you want to use for the installation must be a member of the Administrators group.
- The examples in the scenario use the my_domain\my_account account (which is also a member of the Administrators group) to install CA Server Automation.

Create a Database User With the dbcreator Role

Create a database user for CA Server Automation that you want to use during the product installation and apply the dbcreator role to this user. After the installation, CA Server Automation can use the same user with the appropriate User Mapping settings.

Windows Authentication

Follow these steps:

1. Log in the system using my_domain\my_account or the local system administrator.
2. Log in SQL Server using administrator (sa) permissions or the local system administrator.
3. Expand the Security folder in the navigation tree.
4. Right-click the Logins folder and select New Login ...

   The New Login dialog opens.
5. Under the General section, specify the following settings:
   - Select Windows Authentication.
   - Click Search, enter a login name, for example, my_account, click Check Names.
   - Verify the resolved account my_domain\my_account in the dialog.
6. Change to the Server Roles section, add the dbcreator role, and click OK.

   The new database user has sufficient privileges to install the product.

SQL Server Authentication

Follow these steps:

1. Log in the system using my_domain\my_account or the local system administrator.
2. Log in SQL Server using administrator (sa) permissions.
3. Expand the Security folder in the navigation tree.
4. Right-click the Logins folder and select New Login ...

   The New Login dialog opens.
5. Under the General section, specify the following settings:
   - Enter a login name, for example, causer.
   - Select SQL Server authentication and enter the password for this user.
   - Uncheck "User must change password at next login".
6. Change to the Server Roles section, add the dbcreator role, and click OK.

   The new database user has sufficient privileges to install the product.

Install the Product Using the New Database User

You can install the product using the new database user.

Windows Authentication

Follow these steps:

1. Log in the system using my_domain\my_account.
2. Open Windows Explorer, navigate to the DVD\Windows\Installers directory, right-click install.exe, and select "Run as administrator" to start the CA Server Automation installation wizard.
3. In the Required Configuration dialog, click the Database entry.

   The database configuration dialog opens.
4. Select "Windows Authentication" (default).
5. Specify a database instance if necessary.
6. Uncheck "Use Local System Account" in the "Windows Authentication - Apache" section.
7. Enter the new user name (my_domain\my_account) and password.
8. Check "Grant logon as a Service", and click OK.
9. Follow the instructions of the installation wizard and start the installation.
10. After a successful installation, click Start (Windows), Administrative Tools, Services.

    The Services window opens.
11. Scroll down to CAAIPApache and CAAIPTomcat and stop the services.

SQL Server Authentication

Follow these steps:

1. Log in the system using my_domain\my_account or the local system administrator.
2. Start the product installer of CA Server Automation and start the installation wizard.

   If you are not the local system administrator, open Windows Explorer, navigate to the DVD\Windows\Installers directory. Right-click install.exe, and select "Run as administrator" to start the installation wizard.
3. In the Required Configuration dialog, click the Database entry.

   The database configuration dialog opens.
4. Select "SQL Authentication."
5. Specify a database instance if necessary.
6. Enter the new user name (causer) and password, and click OK.

7. Follow the instructions of the installation wizard and start the installation.
8. After a successful installation, click Start (Windows), Administrative Tools, Services.

   The Services window opens.
9. Scroll down to CAAIPApache and CAAIPTomcat and stop the services.

Change the Owner of the aom2 and dpm Databases

The CA Server Automation installation creates two databases: dpm and aom2. Change the database ownerships to the sa user or to the local administrator.

Windows Authentication

Follow these steps:

1. Log in SQL Server using administrator (sa) permissions or the local system administrator.
2. Click New Query.

   The SQL console opens.
3. Enter the following SQL commands:

   ```
   use dpm
   exec sp_changedbowner 'system\administrator', 'true'
   use aom2
   exec sp_changedbowner 'system\administrator', 'true'
   ```
4. Click Execute.

   The local system administrator owns the aom2 and dpm databases.

SQL Server Authentication

Follow these steps:

1. Log in SQL Server using administrator (sa) permissions.
2. Click New Query.

   The SQL console opens.
3. Enter the following SQL commands:

   ```
   use dpm
   exec sp_changedbowner 'sa', 'true'
   use aom2
   exec sp_changedbowner 'sa', 'true'
   ```
4. Click Execute.

   The sa user owns the aom2 and dpm databases.

Adjust the Permissions of the New Database User to the Required Minimum

CA Server Automation requires a database user with sufficient permissions to use the aom2 and dpm databases. This procedure describes how to adjust these permissions to a minimum.

Windows Authentication

Follow these steps:

1. Log in SQL Server using administrator (sa) permissions or the local system administrator.
2. In the SQL Server Management Studio, expand Security, Logins in the Object Explorer.
3. Right-click the new user (for example, my_domain\my_account) and open Properties, User Mappings.

   The User Mapping dialog appears.
4. Select the aom2 database in the dialog and assign db_datareader and db_datawriter role memberships.
5. Select the dpm databases in the dialog and assign db_datareader and db_datawriter role memberships. Click OK.
6. Click New Query.

   The SQL console opens.
7. To allow the new database user (my_domain\my_account) the execution of stored procedures, enter the following SQL commands:

   ```
   use dpm
   GRANT EXECUTE TO "my_domain\my_account"
   use aom2
   GRANT EXECUTE TO "my_domain\my_account"
   ```
8. Click Execute.
9. Right-click the new user (my_domain\my_account) in the Object Explorer and open Properties, Server Roles.

   The Server Roles dialog appears.
10. Remove the dbcreator role and click OK.

    The new database user provides sufficient permissions to CA Server Automation to use the aom2 and dpm databases.

SQL Server Authentication

Follow these steps:

1. Log in SQL Server using administrator (sa) permissions.
2. In the SQL Server Management Studio, expand Security, Logins in the Object Explorer.
3. Right-click the new user (for example, causer) and open Properties, User Mappings.

   The User Mapping dialog appears.
4. Select the aom2 and dpm databases in the dialog and assign db_datareader and db_datawriter role memberships to both databases. Click OK.
5. Click New Query.

   The SQL console opens.
6. To allow the new database user (causer) the execution of stored procedures, enter the following SQL commands:

```
use dpm
GRANT EXECUTE TO causer
use aom2
GRANT EXECUTE TO causer
```

7. Click Execute.
8. Right-click the new user (causer) in the Object Explorer and open Properties, Server Roles.

   The Server Roles dialog appears.
9. Remove the dbcreator role and click OK.

   The new database user provides sufficient permissions to CA Server Automation to use the aom2 and dpm databases.

Log in the User Interface and Manage Your Environments

Before you can use the CA Server Automation user interface, start the CAAIPApache and CAAIPTomcat services.

Follow these steps:

1. Click Start (Windows), Administrative Tools, Services.

   The Services window opens.
2. Scroll down to CAAIPApache and CAAIPTomcat and start the services.

   After a successful start of the services, CA Server Automation is ready to use.
3. Start the CA Server Automation user interface and manage your environment.

(Optional) Consider the SQL Server User Permissions when Upgrading the Product

The previously described SQL Server user permissions must include the db_owner role membership to support the upgrade of CA Server Automation.

Verify, that the system\administrator or sa database user has the following permission:

- db_owner role membership for aom2 and dpm databases

The SQL Server user for CA Server Automation is specified through the installation wizard and depends on the selection of SQL Server Authentication or Windows Authentication. The SQL Server user requires at least the following permissions for aom2 and dpm databases to support an upgrade:

- db_datareader role membership
- db_datawriter role membership
- EXECUTE permission
- db_owner role membership

After a successful upgrade, you can remove the db_owner role membership from the database user, because it is not required for normal operations.

Chapter 3: Install the Software

This section contains the following topics:

Start the Installation Wizard

Follow these steps:

1. Access the installation media.
2. Navigate to the *drive:*DVD1.
3. Click setup.hta.
4. Click Install CA Server Automation and follow the wizard.

   Note: If you use CA EEM 12.0, verify that you have the "EEM Application User" and "EEM System User" specified before you configure CA EEM in the installation wizard. In the CA EEM Configuration dialog of the installation wizard, enable "Use Existing Security". Add the EEM Application User, EEM System User, and passwords that you have already specified in CA EEM.

   After the installation completes, a record of the installation is created in: *install_path*\log\install. The file, install.log, contains all output and errors; install_error_detected.log is generated for specific error conditions.

   Note: Passwords that are entered during installation are temporarily stored on the hard disk in unencrypted format; they are removed before the installation exits.

Start a Silent Installation

A silent installation consists of editing property files and starting the installation from a command line.

Important! The properties file must use UTF-8 encoding. Unicode and ANSI encoding are not supported.

Follow these steps:

1. Navigate to the root directory of the installation media and copy all folders to the installation server.

   Important! Preserve the directory structure on the installation media when copying the files to the installation server.

2. Open the *path*\ResponseFileTemplates folder on your server.
3. Open and edit the silent.properties file using a text editor.

   Note: Do not remove sections that are unused.

4. Open a Command Prompt window, navigate to the Windows folder, and enter the following command:

   `install.exe -i silent -f <path_to_silent.properties_file>\silent.properties`

5. Review the Install.log file for errors and warnings after installation.

Communication Ports

CA Server Automation requires that multiple ports are open to function properly. If a distributed installation ranges across firewalls, you can use this list to verify that the required communication ports are open.

Active Directory and Exchange Server (ADES)

PowerShell Ports: 80, 443, 5985, and 5986

ADSI Ports: 3268, 389

Amazon EC2 Server

Default Port: 8443

Apache Server

HTTPS Port: 443

CA EEM Server

iGateway Port: 5250

SystemEDGE

UDP Port: 161 (SNMP Get/Set Requests); alternative port: 1691

UDP Trap Port: 162 (Outbound)

SystemEDGE in Managed Mode uses CAM:

CAM UDP Port: 4104

CAM TCP Port: 4105

CA Configuration Automation Server

HTTP/HTTPS Port: 8080

CA Process Automation Server

HTTP/HTTPS Port: 8080

CA Systems Performance LiteAgent

CAM UDP Port: 4104

CAM TCP Port: 4105

Cisco UCS

HTTP Port: 80

HTTPS Port: 443

Citrix XenDesktop

WinRM Port: 5985, 5986

SNMP Port: 161

WMI Port: 135

Citrix XenServer

HTTPS Port: 443

SNMP Port: 161

Huawei GalaX

HTTP Port: 8773

Hyper-V and SCVMM

WMI Port: 135

IBM PowerHA

Secure Shell TCP Port: 22

IBM PowerVM

Secure Shell TCP Port: 22

Kernel-based Virtual Machines (KVM)

REST API Port: 8443

Key Performance Database (KPDB)

Default HTTP Port: 8555

Microsoft SQL Server

Management DB TCP Port: 1433

Performance DB TCP Port: 1433

MSCS AIM

Windows RPC Endpoint Mapper Port: 135

DCOM/WMI Port: dynamically assigned during RPC Endpoint negotiation

For more information, see The default dynamic port range for TCP/IP http://support.microsoft.com/kb/929851.

Oracle Solaris Zones

Secure Shell TCP Port: 22

Orchestrator Port

Default Port: 7889

Policy Configuration

CAM UDP Port: 4104 (Inbound/Outbound)

CAM TCP Port: 4105 (Inbound)

Red Hat Enterprise Virtualization Server

Default Port: 8443

Remote Deployment (Windows)

CIFS UDP Port: 137 (Inbound/Outbound)

CIFS UDP Port: 138 (Inbound/Outbound)

TCP Port: 135 (Inbound)

CIFS TCP Port: 139 (Inbound/Outbound)

CIFS TCP Port: 445 (Inbound/Outbound)

CAM UDP Port: 4104 (Inbound/Outbound)

CAM TCP Port: 4105 (Configurable)

Remote Deployment (UNIX, Linux)

CAM UDP Port: 4104 (Inbound/Outbound)

Secure Shell TCP Port: 22 (Inbound)

TCP Port: 135 (Inbound)

CAM TCP Port: 4105 (Configurable)

Remote Monitoring AIM

Windows RPC Endpoint Mapper Port: 135

DCOM/WMI Port: dynamically assigned during RPC Endpoint negotiation

For more information, see The default dynamic port range for TCP/IP http://support.microsoft.com/kb/929851.

Self-Service Portal Information

Liferay Tomcat Server Port: 8445

Liferay Tomcat Server Shutdown Port: 8007

SNMP Stack

UDP Ports: 161, 1691, 162 (Trap, Inbound)

Software Delivery

HTTP/HTTPS Port: 80

Storage Servers

NetApp HTTP Port: 8088

NetApp HTTPS Port: 8488

EMC SMI-S HTTP Port: 5988

EMC SMI-S HTTPS Port: 5989

HP SMI-S HTTP Port: 5988

HP SMI-S HTTPS Port: 5989

IBM SMI-S HTTPS Port: 5989

Support Agent

Default HTTP Port: 8556

Tomcat (User Interface)

HTTPS Port: 8443

Shutdown Port: 8005

VMware vCenter

HTTPS Port: 443

VMware vCloud

REST API Port: 8443

Start the User Interfaces and Documentation

After a successful installation, you can start the user interfaces and review the product documentation.

Follow these steps:

1. Review the *Release Notes* for browser requirements.
2. Select Windows Start, Programs, CA, CA Server Automation, Launch CA Server Automation, or enter the URL in a supported browser:
   - CA Server Automation

     Format: https://<localhost | *ip_address*>:*port*/UI

     Example: https://laroo-vm0002:8443/UI
   - Reservation Manager

     Format: https://<*server* | *ip_address* | localhost >:*port*/ssrm

     Example: https://laroo-vm0002:8443/ssrm
3. Use the CA EEM credentials that are specified during installation (application, server, or system user) and click Login.

   Note: CA EEM credentials are valid for CA Server Automation, which includes Self-Service Portal and Reservation Manager.

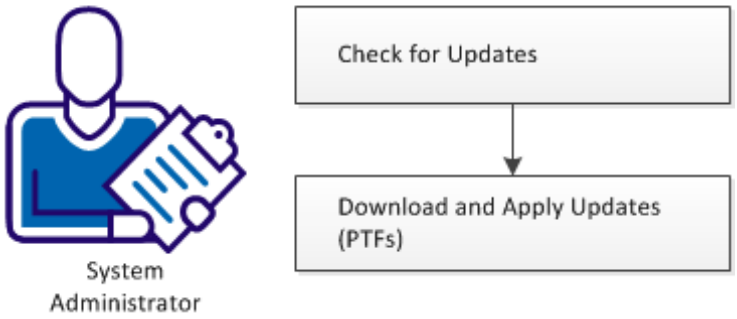
   Note: If you receive a security certificate request, bypass it and continue. To eliminate these messages, acquire a certificate from the vendor of your choice and apply it to the server. For information about installing security certificates, see the Apache Tomcat website.

To start the documentation and online help, select Windows Start, Programs, CA, CA Server Automation, Bookshelf.

How to Update CA Server Automation

As a System Administrator, your job includes applying the PTFs (program temporary fix) for CA Server Automation on manager systems. Applying the PTFs includes downloading and installing the PTFs that you can handle through one application.

How to Apply Updates (PTFs)



Follow these steps:

1. Check for Updates (see page 27).
2. Download and Apply the Updates (PTFs) (see page 28).

Check for Updates

Before you download and apply updates, verify if appropriate updates for this release are available.

Follow these steps:

1. Right-click the icon in the system tray and click "Check for updates".

   The tooltip displays the result.

Additionally, you can specify the settings when to check for updates automatically.

Follow these steps:

1. Right-click the icon in the system tray and click "Settings".

   The Settings dialog appears.
2. Specify the fields in the dialog and click OK.

   The "Check for updates" schedule is set.

Download and Apply the Updates (PTFs)

Download and apply the PTFs to keep the CA Server Automation up-to-date on the manager system.

Follow these steps:

1. Go to Start, All Programs, CA, CA Server Automation, and click CA Server Automation Update.

   The "Updates for CA Server Automation" window is displayed.

2. Open the Applicable page.

   The applicable PTFs for this release are listed.

3. Select the PTFs that you require, click Download selected updates, and then click Apply all downloaded updates.

   The update utility downloads the PTFs to the %INSTALL_PATH%*productname*\CAPTFS directory and starts the application process. The application progress dialog displays the status.

4. After the PTFs are applied successfully, exit the application progress dialog.

   The applied PTFs are listed in the Applied page of the "Updates for CA Server Automation" window.

5. Click Exit.

Chapter 4: Upgrade the Software

This section contains the following topics:

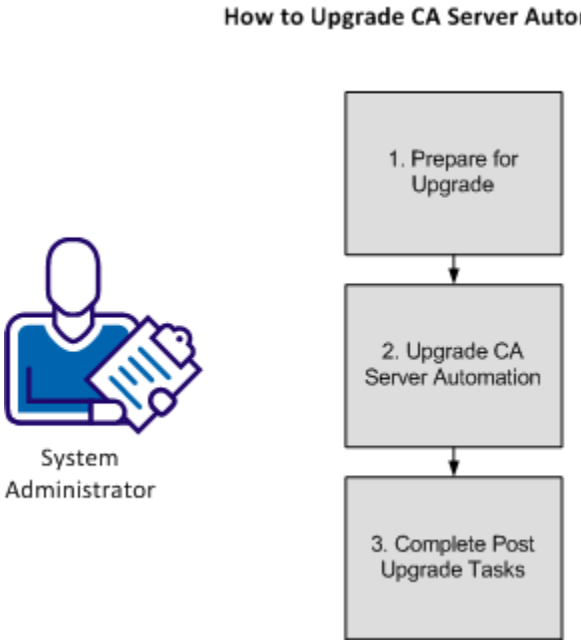
How to Upgrade CA Server Automation

System Administrators use the installation wizard to upgrade CA Server Automation. You can upgrade only core CA Server Automation components (for example, CA EEM and Apache). The upgrade wizard validates required versions of software and optionally lets you install patches.

Note: The upgrade wizard does not upgrade CA integration products (for example, CA ITCM and CA Process Automation). CA integration products require a migration process after upgrading core components.

Note: During upgrade, only the locale used in the previous version is supported. New locale support cannot be added during upgrade.

The following illustration shows the process for upgrading CA Server Automation:



1. Prepare for upgrade (see page 30).
2. Upgrade CA Server Automation (see page 31).
3. Complete post upgrade tasks (see page 32).

Prepare for Upgrade

Upgrading requires that your existing CA Server Automation environment is working and credentials are valid.

Important! Do not uninstall CA Server Automation to upgrade.

Note: CA Server Automation Releases 12.6 supports Microsoft SQL Server 2005 SP3 (32 bit, 64 bit), Standard and Enterprise Editions, SP4 optional and Windows Server 2003 SP2 and 2003 R2 SP2 Standard, Enterprise, and Datacenter Edition (x86, x64). These versions are **not** supported in CA Server Automation Release 12.8.1. During installation, your hardware and software versions are verified. If the versions do not meet the minimal requirements, the installation cannot proceed. For details about supported versions, see the *Release Notes.*

You can upgrade from the previous two releases, excluding any 11.x releases.

If You Are Upgrading From...	Then	Example
CA Server Automation Release 12.6, 12.7, or 12.7.1.	Use the upgrade wizard.	If the current release is Release 12.8.1, you can upgrade directly to Release 12.8.1.
CA Server Automation Release 12.0.2 or 12.5.	Use the upgrade wizard, to move to an interim release, then upgrade to the current release.	If you have Release 12.0.2, upgrade to 12.6 - 12.7, then upgrade to Release 12.8.1.
11.x	Contact Customer Support.	

Complete the following tasks to prepare for an upgrade:

- Back up your existing system.
- Stop all administrative activities and log out the CA Server Automation user interface.
- If you are using Reservation Manager, suspend all activities, including user reservations.

  Note: If reservations are in process as the upgrade starts, you may need to reinitiate reservations. For more information about reinitiating reservations, see the *Administration Guide*.
- Uninstall all instances of CA Software Delivery on remote servers.

  Important! When uninstalling instances, do not select the options to remove the CA EEM AIP instance or the Management and Performance Databases. Uninstalling these items results in a failure to successfully upgrade.

  Note: CA Server Automation Release 12.8.1 installs the adapter for CA Software Delivery on the CA Server Automation node and all configurations are saved in the database.
- Stop the following Windows services:

  1. CAAIPApache
  2. CA Message Queuing Server (ActiveMQ)
  3. CALifeRayTomcat
  4. CAAIPTomcat

     Important! If the CAAIPTomcat service cannot be stopped, terminate the associated java.exe process from the task manager. To identify the java.exe process, open the task manager, click "View", "Select column ...", and select "Image Path Name". The java.exe process that must be terminated is the one with the following path name: *Install_Path**ProductName*\jre\bin\java.exe
- Log in SQL Server with administrator or sa permissions and set the Auto Close parameter for aom2 and dpm databases to False.

Upgrade CA Server Automation

Follow these steps:

1. Access the installation media.
2. Navigate to the *drive:*DVD1.

3. Click setup.hta.
4. Click Install CA Server Automation and follow the wizard.

   After the upgrade completes, a record of the installation is created in: *install_path*\log\install. The file, install.log, contains all output and errors; install_error_detected.log is generated for specific error conditions.

Post Upgrade Tasks

Complete the following tasks after upgrading:

- Restore custom settings for core components.

  The following core components are backed up and renamed during upgrade to product root\component-old:

  - Apache HTTP Server
  - Apache ActiveMQ
  - Apache Tomcat

  If you made custom settings for these services, manually apply them using the backup files.

  Note: SSRM Announcements and Images are automatically carried forward during the upgrade.

- Set chargeback rates for reservations, if applicable. For more information about configuring chargebacks, see the *Administration Guide*.
- Edit any existing SSRM reservation templates for IBM PowerVMs. Increase the maximum number for virtual adapters from 4 to 9.
- Run updates for the following managed systems and servers (if applicable):

  Solaris

  Based on your environment, run the appropriate command:

  1. Navigate to the DVD2\Installers\Solaris_sparc\JumpStart directory and run ca-jumpstart-adapter.Solaris.
  2. Navigate to the DVD2\Installers\Solaris_x86\JumpStart directory and run ca-jumpstart-adapter.SolarisIntel.

  AIX:

  1. Navigate to the DVD2\Installers\AIX_aix\NIM directory and run ca-nim-adapter.AIX.

- (Optional) Upgrade SystemEDGE using the installation wizard.

  For detailed upgrade information, see the *SystemEDGE User Guide.*

- After a product upgrade, some functions of Service Provisioning and Self-Service Portal also require a manual upgrade for full functionality. In the CA Server Automation First Step Dashboard, click the Upgrade Contents link, and select whether to replace your existing templates with new ones, or retain the previous set and also load the new set.

Upgrade the Performance Data

After you upgraded CA Server Automation to Release 12.8.1, upgrade your performance data. To preserve your utilization history, export and import your performance data using the *dpmkpdb.exe* CLI utility.

Note: For more information about the dpmkpdb.exe utility, see the *Reference Guide*.

Follow these steps:

1. Export the performance data from the collection engine:

   `dpmkpdb.exe export_ce -ws_user` *`username`* `-ws_password` *`password`* `-output` *`export.txt`*

2. Import data to KPDB:

   `dpmkpdb.exe import -ws_user` *`username`* `-ws_password` *`password`* `-input` *`export.txt`*

User Resources

After an upgrade from CA Server Automation 12.6 or 12.7, systems, storage, and services that are provisioned in these releases do not appear under Data Center, User Resources. The upgrade process cannot consider these resources, because the information about the users who provisioned these resources is not available in release 12.6 or 12.7.

The User Resources tab was introduced in release 12.7.1 to provide tables for Systems, Services, and Storage. These tables list the properties of the resources and the names of the users that provisioned them.

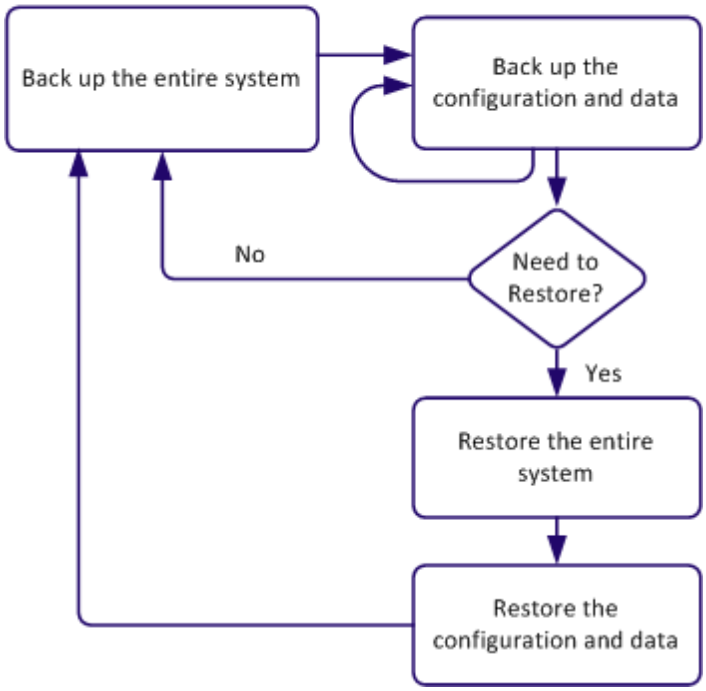
Chapter 5: Backup and Restore

This section contains the following topics:

Backup and Restore Overview

The following sections provide information about the two modes of backup and their corresponding restore processes. The diagram illustrates the procedures required to restore your environments.

Backup and Restore Process



To back up and recover your systems, do the following:

1. Back up the entire system (see page 36) according to your needs.
2. Back up the configuration and data. (see page 37)
3. If you want to restore your system:
   a. Restore the entire system. (see page 41)
   b. Restore the configuration and data. (see page 41)

Back up the Entire System

We recommend performing the entire system (full) backup for disaster recovery at least once a week for the manager nodes. A manager node is any server that has the following components:

- Domain Server
- Distribution Server
- Databases
- EEM server

Back up the manager nodes using an industry standard tool (for example, ARCserve for Physical servers or Snapshots for Virtual Machines). If you have more than one manager node, verify that the backup is performed simultaneously on all the servers.

We recommend that the backup is done offline when there is no user activity. Verify that any active jobs for Remote Deployment are complete before you start the backup.

Note: As Disaster Recovery is for an entire system, consult other product owners who have software on the systems.

Follow these steps:

1. Navigate to Resources, Deploy pane, Jobs and verify that all jobs are 100 percent complete.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server

3. Do *one* of the following:
   - Take a snapshot of the entire manager system.
   - Take a ghost image of the entire manager system.
4. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Back up the Configuration and Data

This section provides the recommendation for incremental backup of the databases, key configuration files, and other data. We recommend that the differential backup is performed at least once a day when the usage is off-peak or the system can be offline.

This section describes the following procedures:

- Back up the Databases (see page 37)
- Back up the Directories and Data (see page 38)

Back up the Databases

SQL Management Studio enables you to back up the Management and Performance Databases.

Follow these steps:

1. Launch the SQL Server Management Studio.
2. Expand the registered SQL Server where AOM2 and DPM databases reside.
3. Expand Databases.
4. Right-click the database, click Tasks, then Back Up.
5. Verify that the Backup type is set to Full and identify the path to where the backup is made.
6. Click OK.

The following table presents the recommendations for the Performance and Management Databases:

Database	Description	Recommendation
AOM2	Management Database	Incremental backup
DPM	Performance Database	The Performance Database contains performance metrics collected by the agents. Unless this data is deemed critical from a historical point of view, it is not recommended to back up this database.

Back up the Directories and Data

We recommend backing up Remote Deployment and Configuration data on a daily basis or according to your company backup policies.

The following table presents the list of key directories, their locations, and the corresponding abbreviations.

Directory	Locating the Directory	Abbreviation
Product Installation Directory* (valid for 32-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\DynamicProvisioningManager" /v InstallDirectory	<INSTALLDIR>
Product Installation Directory* (valid for 64-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\DynamicProvisioningManager"/v InstallDirectory	<INSTALLDIR>
Deployment and Configuration Private Data Directory	Findstr /i "CAISM_PRIVATE_DATA" "<INSTALLDIR>\bin\smglobals.ini"	<PRIVATEDATADIR>

Directory	Locating the Directory	Abbreviation
Deployment and Configuration Public Data Directory	Findstr /i "CAISM_PUBLIC_DATA" "<InstallDir>\bin\smglobals.ini"	<PUBLICDATADIR>
IDManager Install Directory * (valid for 32-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\InfrastructureDeployment" /v MgrApiPath	<IDDIR>
IDManager Install Directory * (valid for 64-bit systems)	REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\InfrastructureDeployment"/v MgrApiPath	<IDDIR>

(*) Note: Use the 32-bit command prompt on 64-bit systems.

The backup recommendations are summarized in the following table:

Description	Directory	Recommendation
Installer configuration file	<INSTALLDIR>\bin\ smglobals.ini	This file defines the CA Server Automation directory settings. Recommended for an incremental backup set.
Domain Server Data	<PRIVATEDATADIR>\ domainserver	Directory and below required for incremental backup except for deployment packages in <PRIVATEDATADIR>\domainserver\Deployment\Packages\SM
Deployment packages	<PRIVATEDATADIR>\ domainserver\ Deployment\ Packages\SM	No need to back up. Can be obtained from installation media.
Distribution Server Data	<PRIVATEDATADIR>\ distributionserver\	No need to back up if backup is done when Domain Server and Distribution Services are stopped.

Description	Directory	Recommendation
IDManager Configuration on the Distribution server	<IDDIR>\config\SM	Required for incremental backup. If this information cannot be backed up on remote distribution servers and the distribution server is reinstalled, reenter credentials during the next deployment using this distribution server.
Web Service Data	<PRIVATEDATADIR>\ caismwebservice	No need to back up. Will be propagated from the domain server.
CA Server Automation Log files	<PUBLICDATADIR>\log	Back up if needed for reference.
ID Log files	<IDDIR>\logs	Back up if needed for reference.

Follow these steps:

1. Verify that all active Remote Deployment jobs are complete.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Back up the recommended directories.
4. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Restore the Entire System

Follow these steps:

1. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
2. Perform the restore using the same backup tool on the same machine that was backed up.

   Important! If you have restored multiple manager nodes, restore all systems to the same backup level to avoid inconsistent data. Restore the manager node with the Domain Server last.
3. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

More Information

Restore the Configuration and Data (see page 41)

Restore the Configuration and Data

After performing the restore of the entire system, restore the differential backup data.

This section describes the following procedures:

- Restore the Databases (see page 42)
- Restore the Directories and Data (see page 43)

More Information

Restore the Entire System (see page 41)

Restore the Databases

When you restore the databases, use SQL Management Studio.

Follow these steps:

1. Shut down the services: CAAIPApache, CAAIPTomcat, CA SM Distribution Server, CA SM Domain Server
2. Launch the SQL Server Management Studio.
3. Expand the registered SQL Server where the database resides.
4. Expand Databases.
5. Right-click the database, click Tasks, then Restore Database.
6. Select the database.
7. Identify the device path from where the restore is made.
8. Click OK.
9. Restart the services: CAAIPApache, CAAIPTomcat, CA SM Distribution Server, CA SM Domain Server

Restore the Directories and Data

Restore the configuration and data files from the same backup media on to the same machine that was backed up.

Follow these steps:

1. Go to Resources, Deploy, Jobs to verify that there are no active Deployment jobs in progress.
2. Stop the following services using *one* of the options:
   - The command-line interface:
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows Service Control Manager:
     - CA SM Domain Server
     - CA SM Distribution Server
3. Restore the configuration and data files from the same backup media.

   Note: The restore operation gets the information back to the same state as at the time of the last backup. Any changes made after the last backup are lost.
4. If multiple manager nodes were backed up, continue to restore other manager nodes.
5. Restart the services that were stopped using *one* of the options:
   - The command-line interface:
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows Service Control Manager.
     - CA SM Domain Server
     - CA SM Distribution Server

Note: If the backup is not performed on the manager node with the Domain Server, stop and start only the Distribution Service.

Appendix A: Troubleshooting

This section contains the following topics:

Customs Views are Lost After Upgrade

Symptom:

After upgrade, my custom views are not working.

Solution:

Your custom views are not lost. See Post Upgrade Tasks (see page 32) to recover.

Installation Problems: General

Symptom:

The installation wizard disappears after the first progress bar, Apache Tomcat does not start, or other installation problems.

Solution:

Systemwide _JAVA_OPTIONS environment variables cause conflicts with CA Server Automation. Unset the variables, or set them at an application level, and restart the installation.

Installation Stops Responding After Remote Desktop Interruption

Symptom:

The installation program stops responding after a Remote Desktop Connection (RDC) interruption. More Command Prompt windows open on the desktop.

Solution:

If you connect to a remote system using RDC and any of the following actions occurred, the installation process stops responding:

- Connection is interrupted during installation.
- CTRL key is intentionally or inadvertently pressed.

To resolve this issue, close any open Command Prompt windows and continue the installation.

Installation Program Continues After Cancellation

Symptom:

If you cancel the installation program before the first installation dialog, the progress bar disappears, the product is not installed, but the installation program continues unpacking files to completion. This process can cause a temporary decrease in CPU performance.

Solution:

When the installation program completes unpacking files, the temporary directory and files are deleted, and the system is unchanged.

Microsoft SQL Server Error

Symptom:

During authentication of the Microsoft SQL Server credentials during installation, a message appears indicating a problem.

Solution:

Verify the following items:

- Your credentials are correct.
- Remote SQL Server instance has TCP/IP enabled.
- Server is listening on the port specified.

Transform Error When Upgrading Windows Server

Symptom:

I am upgrading CA Server Automation to Release 12.8.1 on a Windows 2008 server, which was upgraded from Windows 2003 after the previous CA Server Automation installation. I get the following message:

`Error applying transforms. Verify that the specified transform paths are valid.` *`path`*

Solution:

Before upgrading to Release 12.8.1, you must manually change the Windows 2008 server registry keys. Contact Customer Support.

UNC Path Error When Not Using Built-In Administrator Account

Symptom:

On Windows 2008 R2 when not using a Built-in Administrator account, the install fails with an error message indicating the following errors:

- Drive is a UNC path
- Insufficient permissions exist to execute the install.

This problem occurs if you attempt the install from a mapped drive with a client-defined Administrator.

Solution:

To resolve this issue, perform the following tasks:

1. Open a CMD prompt as the Administrator and run the following commands:

   ```
   Net use Z: \\DVD-IMAGE-PATH
   CD /d Z:
   ```

2. Run the Setup.hta program (right-click the program name and select Run as Administrator).

   Note: On Windows 2008 R2 and later, launch CA Server Automation and any related programs and utilities using the Run as Administrator option.

Index