CA Asset Portfolio Management

Implementation Guide

Release 12.9.00

CA Technologies Product References

This document set references the following CA Technologies brands and products:

- CA Asset Converter
- CA Asset Portfolio Management (CA APM)
- CA Business Intelligence
- CA Client Automation

  (formerly CA IT Client Manager)
- CA Configuration Management Database (CA CMDB)
- CA Embedded Entitlements Manager (CA EEM)
- CA Management Database (CA MDB)
- CA Process Automation™
- CA Service Catalog
- CA Service Desk Manager
- CA Software Asset Manager (CA SAM)
- CA SiteMinder®

This document set also references the following component, which formerly used a different name:

- Common Asset Viewer

  (formerly Asset Management System or AMS)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Introduction

This section contains the following topics:

Overview

This guide provides you with the information you need for a successful CA APM implementation, including information about how to complete the following tasks:

- Plan and prepare for a new installation
- Install and configure the necessary product components
- Integrate with other CA products

Note: You can find the most current version of the Release Notes, which contain the system requirements, at the CA APM product page on CA Support Online.

Audience

This guide is intended for anyone who wants to understand how to install and configure CA APM. The following users have specific tasks to complete using the information in this guide:

- *System administrators* and *administrators* use the information in this guide to install the product for the first time and configure the product based on your implementation requirements.
- *Integrators* use the information in this guide, and their knowledge of CA Technologies products, to integrate CA APM with other CA Technologies products.
- *Users*, when necessary, can use the information in this guide to install the product and components.

To use the information in this guide, have a working knowledge of the Windows operating system and of the basic administrative tasks for your operating system.

CA APM Default Administrator

A default CA APM System Administrator user and role are automatically created during the CA APM installation. This user has complete control over all aspects of the product. The default username and password for the CA APM System Administrator user is uapmadmin.

Note: For security reasons, we recommend that you change the default password during or after the Release 12.9 installation.

After the installation is complete, verify that all services are started. Then, use the login credentials for the CA APM System Administrator user to start the web interface and verify that the product is ready to use.

Chapter 2: Planning

This section contains the following topics:

Installation Planning

To help you plan for a successful CA APM installation, use the following information to research and gather information.

- **Research** - Complete the following steps:
  - Read the Release Notes. Do not start your installation until you have read and understood the information.

    Note: You can find the most current version of the Release Notes on the CA APM product page (Documentation Bookshelves section) on CA Support Online.
  - Verify that you have your installation files.

    Note: If your computer does not have an appropriate drive for the installation media, copy the installation files to the computer where you want to install CA APM. Then, start the installation. For a remote installation over the network, you can also have a shared drive or folder on the network. Then connect over the network to start the installation.
  - Review the certification matrix for a list of third-party software products that have been certified for use with CA APM.

    Note: You can find the most current version of the certification matrix at http://ca.com/support.
  - Consider the network availability, usage bandwidth, and responsiveness.
  - Read about, and have a basic understanding of, the product components (see page 29).
- **Database** - Complete the following steps:
  - Read the *CA Management Database Overview Guide.* Become familiar with the CA MDB. Determine your deployment strategy and become aware of any SQL Server or Oracle issues that you must address to use the CA MDB.
  - Decide which database (either SQL Server or Oracle) to use with CA APM and install the database.

- Configure Oracle or SQL Server.
- (SQL Server) Verify that SQL Server Client Tools are installed on all servers that access the SQL Server database.
- (Oracle) Verify that 32-bit Oracle Client Tools are installed on all servers that access the Oracle database.

Note: We do not recommend the installation of CA APM components, except the CA MDB, on a 64-bit computer that hosts a 64-bit Oracle database server.

- **CA Business Intelligence** - Install CA Business Intelligence and record the login credentials and connection information. Verify the CA Business Intelligence installation (see page 25).

  Note: For more information about implementing CA Business Intelligence, see the *CA Business Intelligence Implementation Guide*.

- **Internet Information Services (IIS)** - Verify that Internet Information Services is installed on all application and web servers (see page 13).

- **CA EEM -** Install CA EEM 12.51. You can install CA EEM using the installer program available on the CA APM installation media.

  Note: If you have a previous version of CA EEM, upgrade to Release 12.51 using the CA EEM installer.

  CA iTechnology iGateway, which is installed with CA EEM, is a shared component that various CA Technologies products use. CA iTechnology iGateway is a web server that sends requests and receives replies using the http protocol.

  CA iTechnology iGateway can be installed with other products also. If CA iTechnology iGateway exists on the computer where you are installing CA EEM, determine if it is 32-bit or 64-bit. If CA iTechnology iGateway and your CA EEM 12.51 server are both 32-bit or both 64-bit, no action is necessary. However, if the two products do not match (for example, one is 32-bit and the other is 64-bit), remove CA iTechnology iGateway (see page 13). Then start the CA EEM installation. The correct version of CA iTechnology iGateway is installed when you complete the CA EEM installation.

- **Common Asset Viewer** - Before you install CA APM, install the Java Development Kit (JDK) (see page 14) on the application server on which you are installing the Common Asset Viewer.

- **CA Software Compliance Manager (CA SCM)** - If you are integrating CA SCM Release 12.6 with CA APM Release 12.9, install CA SCM (and any cumulative releases) before you install CA APM.

- **Pentaho Data Integration (Kettle)** - Install Pentaho Data Integration (Kettle) 4.x before or after you install CA APM. Install Kettle on the local computer where you are installing CA APM. Kettle is required for the Migration Toolkit, which you use to migrate Release 11.3.4 data.

  Note: Kettle is required only if you are upgrading from Release 11.3.4 to Release 12.9 or if you previously upgraded from Release 11.3.4 to Release 12.8.

Verify the Internet Information Services Installation

Before you begin the CA APM installation, verify that Internet Information Services (IIS) 7.0, 7.5, or 8.0 is installed on all application and web servers. If the service is not on a server, add the service before you begin the installation.

Follow these steps:

1. For each application and web server, log in to the server.
2. Open the Control Panel (Administrative Tools, Services).
3. Verify that the IIS Admin service is on the server.

Remove CA iTechnology iGateway

CA iTechnology iGateway, which is installed with CA EEM, is a shared component that various CA Technologies products use. CA iTechnology iGateway is a web server that sends requests and receives replies using the http protocol.

CA iTechnology iGateway can be installed with other products also. If CA iTechnology iGateway exists on the computer where you are installing CA EEM, determine if it is 32-bit or 64-bit. If CA iTechnology iGateway and your CA EEM 12.51 server are both 32-bit or both 64-bit, no action is necessary. However, if the two products do not match (for example, one is 32-bit and the other is 64-bit), remove CA iTechnology iGateway. Then start the CA EEM installation. The correct version of CA iTechnology iGateway is installed when you complete the CA EEM installation.

Note: Various CA Technologies products or components install the 64-bit version of CA iTechnology iGateway, including the 64-bit CA Technologies eTrustITM agent.

Follow these steps:

1. On the computer where you are installing CA EEM, remove CA iTechnology iGateway.

   Note: To uninstall CA iTechnology iGateway successfully, first uninstall all products that are dependent on CA iTechnology iGateway.

   a. Open the Control Panel (for example, click Start, Settings, Control Panel).

   b. Double-click Add or Remove Programs.

   c. Select CA iTechnology iGateway and click Remove.

2. Remove the iGateway and iTechnology registry key folders from the following location:

   HKEY_*localmachine*\SOFTWARE\ComputerAssociates\

3. Delete the IGW_LOC environment variable.
   a. From the Start menu, right-click My Computer and select Properties.
   b. Click the Advanced tab.
   c. Click Environment Variables.
   d. Select IGW_LOC in the System variables list, click Delete, and click OK.
4. Restart the computer.
5. Install CA APM.
6. When the CA APM installation is complete, reinstall the uninstalled components on the computer where CA EEM is installed.

Note: We do not recommend the installation of the CA APM components, except the CA MDB, on a 64-bit computer that hosts a 64-bit Oracle database server.

Install the Java Development Kit (JDK)

Before you begin the CA APM installation, install the Java Development Kit (JDK) 1.7.0_40 (32-bit) on the application server on which you are installing the Common Asset Viewer. The CA APM installation automatically installs the Common Asset Viewer on the application server.

Follow these steps:

1. Log in to the application server.
2. In a web browser, download and install the JDK 1.7.0_40 (32-bit) from the Oracle website (http://www.oracle.com).
3. Set the JAVA_HOME environment variable to reference the JDK 1.7.0.40 (32-bit) installation directory.
4. Update the Path environment variable to reference the \bin directory of the JDK 1.7.0_40 (32-bit) installation directory.

Install Pentaho Data Integration (Kettle)

Install Pentaho Data Integration (Kettle) 4.x on the local computer where you install CA APM. Kettle is required only if you are upgrading from Release 11.3.4 to Release 12.9 or if you previously upgraded from Release 11.3.4 to Release 12.8.

Note: You can install Kettle before or after installing CA APM. However, we recommend that you install Kettle 4.x before you install CA APM.

Follow these steps:

1. Log in as the administrator to the computer where you are installing CA APM.
2. Download Kettle from the CA Support website and install Kettle on the server where you install CA APM Release 12.9. Complete the following steps to download Kettle:
   a. Click the following link:

      ftp://ftp.ca.com/pub/ca_itam/ca_apm/apm12_8/pentaho-kettle-4.4.0.zip

   b. Save pentaho-kettle-4.4.0.zip in the desired directory.

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

   c. Extract the contents of pentaho-kettle-4.4.0.zip.

      A new folder named Kettle is created. Note the path of the folder.
3. Create an environment variable for Kettle by completing these steps.
   a. Click Start, Run, and type sysdm.cpl to access System Properties.
   b. Click the Advanced tab.
   c. Click Environment Variables.
   d. Click New in the System variables section and enter the following details:

      Variable Name

      KETTLE_HOME

      Variable value

      Path of the Kettle folder.

      Note: Ensure the path is set to the parent folder that contains the "data-integration" folder, for example, C:\Program Files (x86)\CA\ITAM\Kettle.

   a. Click OK and exit System Properties.

Retain the Migration Status from Release 12.8

The Migration Utility moves CA APM data objects from Release 11.3.4 to the current release. The migration status (for example, Completed) of each object is displayed on the Migration Utility. If you previously migrated Release 11.3.4 data to Release 12.8, you can migrate objects with Release 12.9 that you could not migrate in Release 12.8. However, to retain the migration status of the objects that you migrated in Release 12.8, perform the following steps before you upgrade to Release 12.9.

Important! Perform these steps before you uninstall Release 12.8.

Follow these steps:

1. Log in to the server where Release 12.8 is installed.
2. Navigate to the Migration Utility resources folder.

   Example:

   `[ITAM Root Path]\Migration Toolkit\migration-utility\resources\`
3. Open the mu_db_delete.bat file in your preferred text editor (for example, Notepad).
4. Delete the entire contents of the file.
5. Save the mu_db_delete.bat file and close the text editor.

You can now proceed with the Release 12.9 upgrade. The Migration Utility retains the status of the objects that you migrated in Release 12.8.

Note: If you uninstalled Release 12.8 without performing these steps first, you can still proceed with the Release 12.9 installation. When you open the Migration Utility, the objects that you previously migrated display a status of Not Started. Update the status manually. Select an object, right-click, and select Move to Completed.

Uninstall Previous Product Versions

If you install CA APM Release 12.9 on a computer with an older version of the product, the installation updates the database only. The installation does not upgrade CA APM to Release 12.9. Uninstall any older version of CA APM manually first and then install Release 12.9.

Note: Stop the Apache Tomcat Common Asset Viewer service before you uninstall a previous version of the product.

Follow these steps:

1. Back up the Storage folder in your current release. (This step applies only if your current release is any version of Release 12.6, 12.7, or 12.8.)

   a. Navigate to the following location on the application server where the Storage Manager service is installed:

      `[ITAM Root Path]/Storage/`

   b. Copy the contents of the Storage folder and paste them in a secure location (but *not* in any of the ITAM Root Path folders).

   Note: When you have completed the product installation, restore the Storage folder contents. For more information, see Verify the Installation (see page 25).

2. Uninstall the previous release or version of the product.

   Note: For information about uninstalling a previous version of CA APM, see the Implementation Guide for that version.

3. Uninstall the CA SAM Import and Export Service (see page 17) if it was installed in a previous release.

You can now install CA APM Release 12.9.

Note: For information about installing Release 12.9, see Installing (see page 19).

Uninstall the CA SAM Import and Export Service

If you implemented CA APM and CA SAM in a previous release, the CA SAM Import and Export Service component is installed on the CA SAM server. Uninstall the CA SAM Import and Export service from the CA SAM server before you install Release 12.9.

Follow these steps:

1. Log in to the CA SAM server.
2. From the Start menu, open the Control Panel (for example, click Start, Settings, Control Panel).
3. Click Programs and Features.
4. Double-click CA ITAM SAM Import Export Service.
5. Follow the on-screen instructions in the uninstallation process.

Chapter 3: Installing

This section contains the following topics:

How to Implement the Software

To implement Release 12.9, complete these steps:

1. Review the prerequisites (see page 19).
2. Install CA APM (see page 20).
3. Update the Apache Tomcat configuration file (see page 21).
4. Start the services (see page 22).
5. Start the web interface (see page 23).
6. Verify the installation (see page 25).

Review the Prerequisites

Before you install Release 12.9, ensure that the computer on which you plan to install meets the minimum system requirements. For more information on system requirements, see the *CA Asset Portfolio Management Release Notes*.

Verify that the following components are installed on the computer where you plan to install the product. The installation process does not start if any of the following components is not installed.

- Microsoft .NET 3.5 Features only on Windows Server 2012
- Microsoft .NET Framework 4.0
- Microsoft WSE 3.0 Runtime

  Note: The installer installs Microsoft .NET Framework 4.0 and Microsoft WSE 3.0 Runtime if it does not detect these components on the computer where you are installing the product.

- Internet Information Services (IIS) 7.0, 7.5, or 8.0
- SQL Server Client or Oracle Client
- Java Development Kit (JDK) 1.7.0_40 (32 bit)

  Note: Set the JAVA_HOME environment variable to the appropriate installation directory.

The installation process starts even if the installer does not detect the following components. However, the installation stops if any configuration you make requires these components.

- Pentaho Data Integration (Kettle) 4.4

  Note: Set the KETTLE_HOME environment variable to the appropriate installation directory.
- CA EEM 12.51
- CA Business Intelligence connectivity

Install CA APM

After you have successfully planned and installed the prerequisite components and products, use the installation media to install CA APM on your local computer. The installer prompts you to enter component and product information to integrate with CA APM. Verify that you are providing the correct information.

Follow these steps:

1. Log in as the administrator to the computer where you plan to install Release 12.9.
2. Open the folder that contains the installation files and double-click the Setup.exe file in the root directory.

   The Installation wizard opens.
3. Follow the on-screen instructions in the wizard.

   Important! Verify that you are providing a valid tablespace path if you have an Oracle database. The database installation fails if this path is invalid. The following path is an example of a valid Oracle tablespace path: C:\app\Administrator\oradata*Oracle_Service_Name*

   Note: In a web farm setup, the CA Business Intelligence Details and CA EEM Details panels do not appear if these components are already installed on one of the servers in the web farm.
4. After the installation is complete, click Finish.

Product Components

During the installation, the installation wizard prompts you to provide information about the following product components. This information includes the server locations and configurations.

- Database server (see page 31)
- Web server (see page 31)
- Application server (see page 32)
- CA EEM (see page 33)
- CA Business Intelligence (see page 33)

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Update the Apache Tomcat Configuration File

The Common Asset Viewer lets you view discovered and owned data for an asset that has been linked through reconciliation. This data includes system configuration, operating system, system devices, and file systems. The Common Asset Viewer requires that you install the Java Development Kit (JDK) (see page 14) before you start the CA APM installation. The Common Asset Viewer also requires the Apache Tomcat server, which is included with the CA APM installation. You can change this value after the installation. You first update the port in the Apache Tomcat configuration file. Then, you change the port in the product (Administration tab, System Configuration, Common Asset Viewer).

Important! The Tomcat port number for CA APM defaults to 9080. If another product that is integrated with CA APM uses this port number, change the port number in CA APM so that you do not have a conflict.

Follow these steps:

1. On the application server where the Common Asset Viewer is installed, navigate to one of the following folders, depending on your server:

   `C:\Program Files\CA\SC\AMS\Tomcat\conf (for 32-bit operating systems)`

   `C:\Program Files (x86)\CA\SC\AMS\Tomcat\conf (for 64-bit operating systems)`

2. Select and open the server.xml file.

3. Navigate to the following section of the server.xml file:

```
<Connector port="9080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
```

4. Update the Tomcat port number with the same number that CA APM uses (Administration tab, System Configuration, Common Asset Viewer).
5. Save the server.xml file.

Start the Services

After the installation is complete, start all services.

Note: In certain circumstances, after the product installation, you can receive a message that CA Business Intelligence was installed but requires you to restart the web server. Restart the web server before verifying that the CA Business Intelligence services are started.

Follow these steps:

1. Open the Control Panel (for example, click Start, Settings, Control Panel).
2. Double-click Administrative Tools.
3. Double-click Services.
4. Locate and start each of the following services:
   - Apache Tomcat Common Asset Viewer
   - CA Asset Portfolio Management - Data Importer Engine
   - CA Asset Portfolio Management - Event Service
   - CA Asset Portfolio Management - Export Service
   - CA Asset Portfolio Management - Registration Service
   - CA Asset Portfolio Management - HW Reconciliation Engine
   - CA Asset Portfolio Management - LDAP Import Service
   - CA CASM

     Important! For performance reasons, we recommend that you do not start the CA CASM service when you do not use multi-tenancy.
   - CA iTechnology iGateway 4.6

5. To verify CA Business Intelligence services with the Central Configuration Manager, select Start, Programs, BusinessObjects XI Release, BusinessObjects Enterprise, Central Configuration Manager.

   The Central Configuration Manager opens.

   If any service is not started, right-click the service and select Start.

Start the Web Interface

After the installation is complete, you can start the web interface to verify that CA APM is ready to use. After you verify that the web interface starts, provide all administrators with the URL and login credentials to log in and prepare the product for users. Administrators can then set up security, configure the user interface, set up hardware reconciliation, and, if necessary, configure the product components. After the administrators prepare the product, they can provide users with the URL and login credentials. For information about administering and preparing the product for users, see the *Administration Guide*.

Note: Before you start the web interface, ensure that you register ASP.NET with IIS (see page 24).

Start the web interface using one of the following methods:

- Open a supported web browser and enter the following URL:

  `http://servername:port/itam`

  Replace servername and port with the name of the server and the port that are hosting the CA APM web servers.

  Note: If the Internet Explorer browser security is set to high, a content warning message appears when you start the web interface. To avoid this message, add the web site to your trusted sites or lower your security settings.

  A Start menu shortcut is created on your web server that references the URL location.

- Click Start, Programs, CA, Asset Portfolio Management, Asset Portfolio Management.

To log in to CA APM, enter the following default credentials:

User Name

uapmadmin

Password

uapmadmin

Note: If you changed the password during the installation, use the password that you created.

In some situations, a browser error or a user name error (see page 148) appears. You can resolve these errors by following the troubleshooting instructions.

Register ASP.NET with IIS

After you install IIS and ASP.NET on the computer where you plan to install CA APM, ensure that you register ASP.NET with IIS.

Follow these steps:

1. On Windows Server 2008, perform the following actions:
   a. In the command prompt, navigate to the appropriate Microsoft.NET framework folder. For example, C:\Windows\Microsoft.Net\Framework64\v4.0.30319 or C:\Windows\Microsoft.Net\Framework\v4.0.30319.
   b. Run the following executable file:

      aspnet_regiis.exe

   ASP.NET is now registered with IIS.
2. On Windows Server 2012, perform the following actions:
   a. Open the Server Manager.
   b. Under the Manage menu, select Add Roles and Features.

      The Add Roles and Features Wizard opens.
   c. Follow the on-screen instructions and select the installation type and the destination server.
   d. In the Select server roles pane, under Roles, expand Application Development and select the appropriate ASP.NET version and click Next.
   e. Follow the on-screen instructions and complete the installation.

   ASP.NET is now registered with IIS.

Verify the Installation

After you have completed all installation procedures, you can verify that Release 12.9 was installed successfully.

Follow these steps:

1. Log in to the servers where you installed CA APM Release 12.9.
2. (Windows Server 2008 or Windows Server 2012) From the Start menu, select Control Panel, Programs and Features.
3. Verify that the following component is available on all applicable servers:

   `CA Asset Portfolio Management`

   You have completed the installation verification.

Note: If you backed up the Storage folder contents before installing Release 12.9, restore the contents now. Use the Storage folder contents that you copied and paste them into the following location:

`[ITAM Root Path]/Storage/`

If you receive a prompt about folders that already exist, merge the folders.

For more information about backing up the Storage folder, see Uninstall Previous Product Versions (see page 16).

Verify the CA Business Intelligence Installation

After you have completed all installation procedures, you can verify that CA Business Intelligence was installed successfully.

Follow these steps:

1. Review the BiConfig.log file.
   a. Navigate to the following folder on the application server where CA APM is installed:

      `[ITAM Root Path]\ITAM\BIAR\biconfig\`

   b. Open the BiConfig.log file in a text editor (for example, Notepad).

c. Search for errors that are related to exporting the BIAR file to the reporting server.

- If no errors exist, CA Business Intelligence was installed successfully. Proceed with Step 3 (Verify CA Business Intelligence on the common home page).
- If an error exists, import the BIAR file manually to the reporting server (proceed with the following steps).

2. Import the BIAR file manually (applicable if errors exist in the log file).

a. Open a command prompt window from the Start menu on the application server where CA APM is installed.

b. Navigate to the following folder:

`[ITAM Root Path]\ITAM\BIAR\biconfig`

c. Open the ItamBoSetup-InstallBiar.xml file in a text editor (for example, Notepad).

- Enter the CA MDB database password.
- Enter the CA Business Intelligence server password.

d. Save and close the ItamBoSetup-InstallBiar.xml file.

e. Execute the following command:

```
biconfig -h CA_Business_Intelligence_server_name -u
CA_Business_Intelligence_admin_user_name
-p CA_Business_Intelligence_admin_password -f ItamBoSetup-InstallBiar.xml
```

f. Open the BiConfig.log file again and verify that CA Business Intelligence was installed successfully.

g. Proceed with Step 3 (Verify CA Business Intelligence on the common home page).

3. Verify CA Business Intelligence on the common home page.

a. Open the common home page from the Start menu (All Programs, CA, Asset Portfolio Management, CA IT Asset Manager).

b. Verify that no warning message is shown regarding CA Business Intelligence.

- If no warning is shown, CA Business Intelligence was installed successfully. You do not need to proceed with the following steps.
- If a warning is shown, verify that the CA Business Intelligence reporting server port is correct (proceed with the following steps).

4. Verify the CA Business Intelligence reporting server port (applicable if the common home page shows a warning).

a. Click Administration, System Configuration on the CA APM user interface.

b. Select Web Server on the left.

c. Verify that the Reporting Server Port field contains the correct value for your implementation.

- If the port value is incorrect, enter the correct value. Restart Internet Information Services (IIS) on the CA APM web servers and application servers by executing the iisreset command.
- If the port value is correct and a warning was shown on the common home page, contact CA Support.

Install the CA SAM Import and Export Service

Install the CA SAM Import and Export Service component on the CA SAM server if you are implementing CA APM and CA SAM.

Note: You do not need to install the CA SAM Import and Export Service if you are not implementing CA SAM as your software asset management system.

Important! Microsoft .NET Framework 4.0 must be installed on the CA SAM server before you install the CA SAM Import and Export Service.

Follow these steps:

1. Log in to the CA SAM server.
2. Navigate to the SAMImportExportSetup folder on the CA APM installation media. Copy the folder and all of its contents to a local folder on the CA SAM server.
3. In the SAMImportExportSetup folder on the CA SAM server, double-click CAITAMSAMImportExportServiceInstaller.msi.

   A prompt for the installation root path appears.
4. Enter the ITAM root path for installing the CA SAM Import and Export Service component.

   The following example shows the recommended path.

   Example:

   C:\Program Files\CA\ITAM

   You have completed installing the CA SAM Import and Export Service.

Secure Network Communication Configuration

After the installation is complete, the product is configured for non-secure network communication (http). You can configure the product for secure network communication (https) by first configuring IIS on the product servers to support the Secure Socket Layer (SSL) protocol. Then you set CA APM configuration parameters for secure network communication.

Complete the following actions:

1. Configure IIS for secure network communication (see page 28).
2. Configure CA APM for secure network communication (see page 28).

Configure IIS for Secure Network Communication

Configure IIS on the product servers to support the Secure Socket Layer (SSL) protocol.

Follow these steps:

1. Launch the Internet Information Services (IIS) Manager on the CA APM web server.
2. Select Server Certificates.
3. Click Create Self-Signed Certificate and specify a certificate name.
4. Select the web site (on the left) where CA APM is installed (for example, Default Web Site).
5. Click Bindings under Actions on the right.

   The Site Bindings dialog opens.
6. Click Add.
7. Select https for the Type.
8. Specify the port and the SSL certificate name.
9. Perform these same steps on the CA APM application server.

Configure CA APM for Secure Network Communication

Configure CA APM on the product servers to support the Secure Socket Layer (SSL) protocol.

Follow these steps:

1. Log in to the product and navigate to Administration, System Configuration.
2. Click Web Server on the left.

3. Change the server protocol to https and click Save.
4. Click WCF Service on the left.
5. Change the server protocol to https and click Save.
6. Click Application Server on the left and select the Show Advanced Options check box to see all configuration parameters.
7. Change the server protocol to https.
8. Change the server port and the component server port to the port of the https protocol (by default, 443) and click Save.
9. Reset IIS on the web server and the application server.

You can now start the product web interface using secure network communication. Open a supported web browser and enter the following URL:

`https://servername/ITAM/Pages/UserLogin.aspx`

Replace *servername* with the name of the server that is hosting the CA APM web server.

Configure Product Components

You can change the component configurations and you can configure additional components after you install the product.

You can configure the following components:

- Web server (see page 31)
- Application server (see page 32)
- Hardware Reconciliation Engine (see page 32)
- CA EEM (see page 33)
- CA Business Intelligence (see page 33)
- Export Service (see page 33)
- Data Importer Engine Service (see page 33)
- Import Driver (see page 34)
- LDAP Data Import and Sync Service (see page 34)
- Storage Manager Service (see page 34)
- CA APM Registration Service (see page 34)
- Common Administration for Service Management (CASM) (see page 35)
- Event Service (see page 35)

- Common Asset Viewer (see page 35)
- WCF Service (see page 36)
- Software Asset Management (see page 36)

Follow these steps:

1. Log in to CA APM as the administrator.
2. Click Administration, System Configuration.
3. On the left, click the product component that you want to configure.
4. Configure the settings and click Save.
5. Recycle the settings in the application pool.

   For more information, see Recycle Settings in the Application Pool (see page 30).
6. Restart the services.

   For more information, see Start the Services (see page 22).

Note: You cannot configure the database server from the System Configuration page. Update the corresponding configuration files for any database server configuration settings.

For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Recycle Settings in the Application Pool

After you configure a product component through System Configuration, recycle the settings in the Application Pool.

Follow these steps:

1. From the Start menu, open the Control Panel.
2. Double-click Administrative Tools and then double-click Internet Information Services (IIS) Manager.
3. In the Connections pane, expand the server name and click Application Pools.
4. In the Application Pools pane, select ITAM.
5. In the Actions Pane, click Stop and then click Start.

Database Server

The database server is a product component that hosts the Oracle or SQL Server database management system for CA APM. The CA MDB is installed on the database server. The application server, Hardware Reconciliation Engine, and other product components retrieve data from and store data in the CA MDB.

The following fields require explanation:

MS SQL Server Instance

Defines the name of the MS SQL Server instance that is being configured. Enter the instance name only when multiple SQL Server named instances exist. Leave the field blank if there is only one (default) instance.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Web Server

The web server is the main server that hosts the web application and builds the CA APM user interface. This server communicates with the user and the application server.

The following fields require explanation:

Web Server or Load Balancer IP/Host

The CA APM installation, by default, sets this field to the web server host name.

- In a single web server environment, you can enter the web server host name, or the web server IP address.
- In a multiple web server environment, you can enter either the web server host name, or the IP address of the Load Balancer.

Note: The web server can be registered with a different name in the Domain Name System (DNS) than what is registered as the web server host name. In this situation, specify the different name in this field.

You can configure additional web server components after you install the product.

Note: For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Application Server

The application server is the server that connects the database server and the web server for CA APM. The business and data access logic reside on the application server. To allow for scalability, the application server and web server are on two distinct servers.

You can have more than one application server. The Export Service component and the Storage Management Service component must be installed on one of the application servers, but not necessarily on the same server.

The following fields require explanation:

Application Server or Load Balancer IP/Host

The CA APM installation, by default, sets this field to the application server host name.

- In a single application server environment, you can enter the application server host name, or the application server IP address.
- In a multiple application server environment, you can enter either the application server host name, or the IP address of the Load Balancer.

Note: The application server can be registered with a different name in the Domain Name System (DNS) than what is registered as the application server host name. In this situation, specify the different name in this field.

You can configure more application server components after you install the product.

Note: For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Hardware Reconciliation Engine

The Hardware Reconciliation Engine is the service that matches discovered assets to their corresponding owned assets from different logical repositories. You can manage the assets based on your business practices. The Hardware Reconciliation Engine retrieves data from and stores the results in the CA MDB. You can install the Hardware Reconciliation Engine on one or more servers.

You can configure more Hardware Reconciliation Engine components after you install the product.

Note: For more information about changing the component configurations and adding servers, see the *Administration Guide*.

CA EEM

CA APM uses CA EEM for authentication. Other products that need CA EEM for authentication can use the same CA EEM server that CA APM uses.

- To manage security centrally for multiple CA Technologies products, specify the name, location, and login credentials for the existing CA EEM server.
- To manage CA APM security independently from other CA Technologies products, install CA EEM on any single application or web server other than the one where the existing CA EEM is installed.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

CA Business Intelligence

CA Business Intelligence administers, monitors, and configures the reporting environment. CA APM uses CA Business Intelligence to integrate, analyze, and present information required for effective enterprise IT management.

For information about the login credentials and connection information that you enter for the CA Business Intelligence component, see How to Integrate CA APM and CA Business Intelligence (see page 102).

Export Service

The Export Service exports data from CA APM and saves the results in formats such as a comma-separated value (CSV) file. To accomplish this task, the Export Service interacts with the Storage Manager Service so that you can specify where the exported files are stored.

Note: For more information about the Export Service, see the *User Guide*.

Data Importer Engine Service

The Data Importer Engine Service imports bulk product information into the CA MDB through column and field mapping.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Import Driver

The Import Driver processes discovered hardware data exports from CA SAM. CA APM uses the discovered hardware data to link ownership and discovery data. CA APM exports ownership data back to CA SAM.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

LDAP Data Import and Sync Service

The LDAP Data Import and Sync Service imports data into CA APM from CA EEM or external data sources (LDAP or CA SiteMinder). Install the LDAP Data Import and Sync Service on one of the Data Importer servers.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Storage Manager Service

The Storage Manager Service stores exported files, attachment files, data import data and map files, and log files for data import and mass change. If your current product release is any version of Release 12.6, 12.7, or 12.8, you must back up the contents of the Storage folder before you uninstall your current release. After you have completed the Release 12.9 installation, restore the contents of the folder. For more information, see Uninstall Previous Product Versions (see page 16).

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

CA APM Registration Service

The CA APM Registration Service consolidates individual CA APM CORA services into one main service. You can have installations of other CA Technologies products that also use the CORA API. The changes that you make to the CORA API in your CA APM environment do not affect the use of the CORA API by other CA Technologies products.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Common Administration for Service Management (CASM)

The Common Administration for Service Management (CASM) provides administrative functionality, such as multi-tenancy administration, to CA APM. Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA APM.

Note: For more information about implementing multi-tenancy, see How to Implement Multi-Tenancy (see page 92).

Event Service

The Event Service manages the events and notifications process in CA APM. Events are important activities or data changes that you want to track and that you define in CA APM. After a defined event has occurred, notifications are sent to alert appropriate users and administrators about the event.

To perform the notification function, the Event Service interacts with a workflow provider (for example, CA Process Automation) using the Web Service. A workflow provider manages automated processes. If your workflow provider is CA Process Automation, you can specify the existing instance of CA Process Automation during the installation. You can also share CA Process Automation with CA Service Desk Manager and CA Service Catalog.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Common Asset Viewer

The Common Asset Viewer lets you view discovered and owned data for an asset that has been linked through reconciliation, including system configuration, operating system, system devices, and file systems. You can view this data on the Asset Details page by clicking the Owned Information or Discovered Information link.

The Common Asset Viewer requires the following components to install and execute successfully:

- Apache Tomcat server, which is included with the CA APM installation. The default value for the Apache Tomcat server port is 9080. You can change this value after the installation. You first update the port in the Apache Tomcat configuration file (see page 21). Then, you change the port in the product (Administration tab, System Configuration, Common Asset Viewer).
- Java Development Kit (JDK). Before you begin the CA APM installation, install the JDK (see page 14) on the application server on which you are installing the Common Asset Viewer.

After you install the Common Asset Viewer, the component is configured for non-secure network communication (http). You can configure the component for secure network communication (https) by first configuring the Apache Tomcat server (where the Common Asset Viewer is installed) to support the Secure Socket Layer (SSL) protocol. Then you need to change a setting for the Common Asset Viewer component in the web configuration file.

Important! The Tomcat port number for CA APM defaults to 9080. If another product that is integrated with CA APM uses this port number, change the port number in CA APM so that you do not have a conflict.

WCF Service

The Windows Communications Foundation (WCF) service implements the web services in CA APM. The web services let you use a standards-based interface to build client applications that integrate with CA APM.

The web services let you create, search, update, copy, and delete CA APM objects from your external client application. Your assigned user role determines whether you have permission to access the web services in CA APM. Your role also restricts the objects and data (classes and attributes) that you can view or modify.

Specify the server name for the WCF Service component. You can modify the WCF Service protocol setting. You can change the configuration of the WCF Service component after you install the product.

Note: For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Software Asset Management

The Software Asset Management component allows you to enable software asset management capabilities through CA SAM. If you implement both CA APM and CA SAM, you can coordinate the management of both hardware and software assets in your organization. CA APM maintains hardware asset data and CA SAM maintains software asset and license data. Common data that both products require is shared.

The product installation does not configure the Software Asset Management component. Configure this component through System Configuration after you install the product.

Note: You can change the component configurations and configure additional components for your enterprise after you install the product. For more information about changing the component configurations and adding servers, see the *Administration Guide*.

Repair CA APM

If you have CA APM installed, you can use the installation program to repair any installation errors. These errors can be related to the product or any of its components.

Follow these steps:

1. Log in as the administrator to the computer where you installed CA APM.
2. Open the folder that contains the installation files and double-click the Setup.exe file in the root directory.

   The installation wizard opens.
3. Click Repair.
4. Follow the on-screen instructions in the repair process.

Uninstall CA APM

You can decide to uninstall CA APM from a computer for various reasons. For example, you can uninstall CA APM because you decided to use the computer for a different purpose or to move the components to another computer.

Follow these steps:

1. Log in as the administrator to the computer where you installed CA APM.
2. Open the folder that contains the installation files and double-click the Setup.exe file in the root directory.

   The installation wizard opens.
3. Click Uninstall.

   The uninstallation starts.
4. Follow the on-screen instructions in the uninstallation process.

Chapter 4: How to Migrate CA APM Data from Release 11.3.4 to Release 12.9

This section contains the following topics:

How to Migrate CA APM Data from Release 11.3.4 to Release 12.9

As a system administrator, you perform the data migration when you want to move CA APM data from Release 11.3.4 to Release 12.9. After you install Release 12.9, the CA Management Database (CA MDB) structures are upgraded and you are prompted to migrate your data.

Important! With Release 12.9, you can migrate objects that were not migrated with Release 12.8. These objects are costs and payments extensions and audits, custom relationships and audits, and relationship extensions and audits. With this release, all relationships are migrated, including custom relationships and relationships that were not product-provided. If you previously migrated your data from Release 11.3.4, you can migrate the data for just these objects. You do not need to perform the complete data migration again.

Installing the upgrade and migrating your data are separate processes:

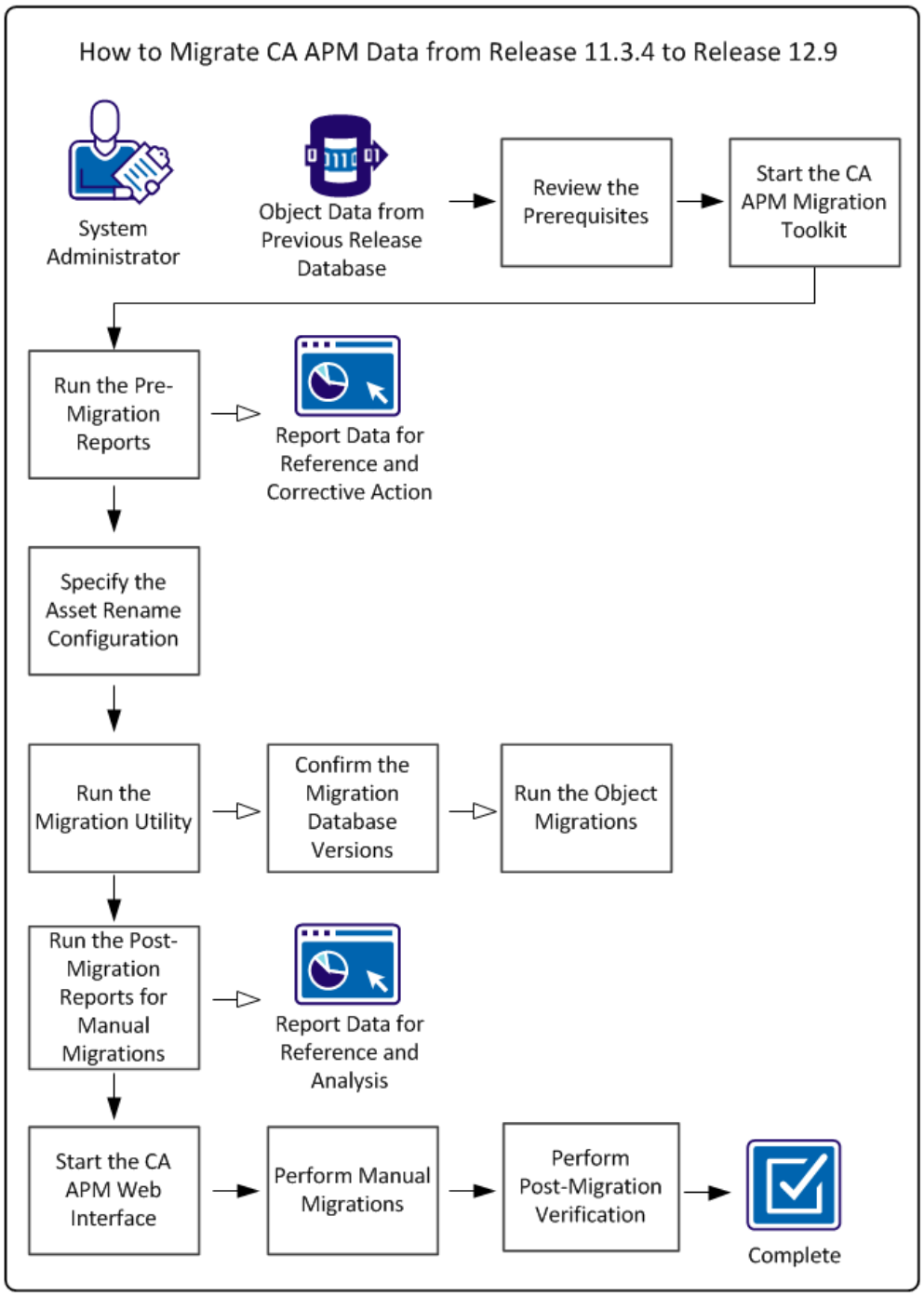
- **Upgrade**. Updates the application and database structures to a newer version.
- **Migrate**. Transforms or moves the data from previous database structures to new database structures, which were created during the upgrade.

The CA APM Migration Toolkit contains the following tools to assist you with migrating your data from Release 11.3.4 database structures to the new Release 12.9 database structures:

- **Migration Documentation**. Provides the instructions for generating the migration reports, running the Migration Utility, and manually migrating objects.
- **Migration Reporting**. Generates reports that help you during the migration process. You generate pre-migration reports (see page 48) *before* you run the Migration Utility (see page 57) to avoid potential problems during the migration. You generate post-migration reports (see page 63) *after* you run the Migration Utility. The post-migration reports help you manually migrate legacy database structures that cannot be migrated using the Migration Utility.

- **Duplicate Asset Name Configurator**. Specifies the renaming configuration to apply to duplicate Asset Names.
- **Migration Utility**. Provides automated steps to move the selected objects in your legacy database structures to new database structures.

The following diagram illustrates how a system administrator migrates data.



To migrate CA APM data, perform these steps:

1. Review the Prerequisites (see page 43).
2. Start the CA APM Migration Toolkit (see page 48).
3. Run the Pre-Migration Reports (see page 48).

   Use the pre-migration report data for reference and corrective action (see page 49).
4. Specify the Asset Rename Configuration (see page 55).
5. Run the Migration Utility (see page 57).
   a. Confirm the Migration Database Versions (see page 59).
   b. Run the Object Migrations (see page 60).
6. Run the Post-Migration Reports for Manual Migrations (see page 63).

   Use the post-migration report data for reference and analysis (see page 64).
7. Start the CA APM Web Interface (see page 68).
8. Perform Manual Migrations (see page 69).
9. Perform Post-Migration Verification (see page 85).

Example: Migrate CA APM Data from Release 11.3.4 to Release 12.9

Miriam is the CA APM system administrator at Document Management Company. She wants to upgrade CA APM Release 11.3.4 to Release 12.9 and migrate the data from legacy data structures to the upgraded data structures. Miriam reviews the prerequisites to start the migration and upgrades to the new release.

Miriam starts the CA APM Migration Toolkit. First, she generates and reviews the pre-migration reports. The reports help identify objects that she has to correct in the legacy data structures before successfully running the Migration Utility. She sets some of the reports aside to use later to configure new names for assets that have the same name and to perform manual migrations.

After Miriam makes the corrections to the legacy data structures, she reviews the Duplicate Asset Name Report to identify non-unique Asset Names. Miriam opens the Duplicate Asset Name Configurator and selects a renaming configuration for duplicate Asset Names. These assets are renamed when Miriam runs the Migration Utility.

Miriam opens the Migration Utility. She tests the database connection, which confirms that the correct CA APM legacy database version is being migrated to the correct new release database version.

Miriam selects the objects to migrate and runs the Migration Utility. She monitors the migration process by reading the progress and status messages. When all of the objects are migrated, the Audit History object becomes available for migration. She selects the Audit History object and reruns the Migration Utility.

When the Migration Utility process finishes, Miriam generates the post-migration reports. The reports specify the data that was successfully migrated and the data that was not migrated. Miriam has to migrate manually the data that was not migrated.

Manual migrations are performed using the upgraded CA APM Release 12.9 web interface. Miriam starts the web interface. She performs the manual migrations using the post-migration report information. She verifies the migrated data to complete the migration process.

Review the Prerequisites

Verify that you have completed these prerequisites in the following order to ensure that you can successfully migrate the data:

Note: Many of the migration prerequisites are completed during the Release 12.9 installation. The *Implementation Guide* provides information about the installation.

1. Read the following information:
   - CA IT Asset Manager Product Roadmap.
   - Differences Between CA IT Asset Manager 12.9 and Prior Releases (CA IT Asset Manager 12 and CA Asset Portfolio Management 11.3.4).
   - Known Issues available on the CA APM product page.
   - Relationship Differences Between Release 11.3.4 and Release 12.9 (see page 45).
2. Ensure that the current Release 11.3.4 patch level is cumulative patch 14 or higher. If the current patch level is unknown, or not cumulative patch 14 or higher, download and apply the latest CA APM Release 11.3.4 cumulative patch from the CA Support website.
3. Download Kettle from the CA Support website and install Kettle on the server where you install CA APM Release 12.9. Complete the following steps to download Kettle:
   a. Click the following link:

      `ftp://ftp.ca.com/pub/ca_itam/ca_apm/apm12_8/pentaho-kettle-4.4.0.zip`

   b. Save pentaho-kettle-4.4.0.zip in the desired directory.

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

   c. Extract the contents of pentaho-kettle-4.4.0.zip.

      A new folder named Kettle is created. Note the path of the folder.

4. Create an environment variable for Kettle by completing these steps.
   a. Click Start, Run, and type sysdm.cpl to access System Properties.
   b. Click the Advanced tab.
   c. Click Environment Variables.
   d. Click New in the System variables section and enter the following details:

      Variable Name

      KETTLE_HOME

      Variable value

      Path of the Kettle folder.

      Note: Ensure the path is set to the parent folder that contains the "data-integration" folder, for example, C:\Program Files (x86)\CA\ITAM\Kettle.

5. Stop the following services and the scheduled tasks for CA APM and other integrated Service Management products:
   - CA Unicenter Asset Portfolio Management (CA APM)
     - CA APM Cache Service
     - CA APM Notification Service
     - Automated reconciliation tasks
   - CA Service Catalog Release 12.8 and Release 12.9
     - CA Service Catalog
     - CA Service Accounting
   - CA Service Catalog Release 12.7
     - CA Service Accounting
     - CA Service Fulfillment
     - CA Service Repository Agent
     - CA Service View
   - CA Service Desk Manager
     - CA Service Desk Manager Server

- CA Client Automation
  - For CA Client Automation Enterprise Managers and Domain Managers that directly share the CA MDB being migrated, stop the CA Client Automation Service using *caf* stop.
  - For other servers running supplemental Engine processes against the CA MDB being migrated, stop the CA Client Automation Service using *caf* stop.
  - For any Engine processes executing the Database Synchronization tasks to the CA MDB being migrated, stop the Database Synchronization jobs using the DSM Explorer.
  - Stop the Engine replication tasks to the Enterprise using the DSM Explorer for each CA Client Automation Domain Manager that reports to the Enterprise.

6. Back up the CA APM Release 11.3.4 database.
7. Locate the CA Migration Health Check Utility in the Health Check Utility folder on the CA APM Release 12.9 installation media. Execute the utility on the CA APM Release 11.3.4 database.

   Important! For information about running the utility, see the *CA Migration Health Check Utility User Guide*, which is available on the installation media.
8. Download the JRE 1.7 from the Oracle website (http://www.oracle.com) and install the JRE on the server where you install CA APM Release 12.9.
9. Review the Microsoft SQL Server Transaction Log Sequence settings for the CA MDB, and ensure that the settings are positioned for bulk loading. Complete the following steps to locate the information:
   a. In a web browser, open the Microsoft website (http://www.microsoft.com) and search for "Transaction Log Management".
   b. Follow the instructions in the article.
10. Install Release 12.9 against the Release 11.3.4 database.

    Note: If you previously migrated Release 11.3.4 data to Release 12.8, you need to perform some steps to retain the migration status of the migrated objects. See the *Implementation Guide* installation planning section for information about how to retain the migration status.
11. Verify that no Release 12.9 services are running. These services can still be running if you exited the CA APM Migration Toolkit before you ran the Data Migration Utility or generated the reports for manual migrations.

Relationship Differences Between Release 11.3.4 and Release 12.9

CA APM Release 11.3.4 includes product-provided relationships and allows you to add new custom relationships. The support for relationships has changed in Release 12.9.

Relationships that Are not Product Provided in Release 12.9

The following relationships and associated links that are provided in Release 11.3.4 are not product provided in Release 12.9. However, these relationships are migrated to custom relationships in Release 12.9.

- Activity Summary
- Contacts (Budget manager, Supported by, User)
- Dependencies (Depends on)
- Product Evolution (Evolved into)
- Product Upgrade (Upgraded to)
- User Allocation (Allocated to)
- SW Allocation (Allocated on)

Product-Provided Relationships in Release 12.9

The following Release 11.3.4 relationships are product provided in Release 12.9:

- Asset Entitlement (Licensed to)
- Company Acquisition (Acquired By)
- Company Entitlement (Licensed to)
- Contact Entitlement (Licensed to)
- Governing Document (Governed by)
- Image Partitions (Partitioned CPU)
- Legal Amendment (Amends)
- Location Entitlement (Licensed to)
- HW Asset Configuration (Generic component, Specific component)
- HW Model Configuration (Generic component)

The data structures to store the relationship information have changed. To move the relationship information from Release 11.3.4 to Release 12.9, the Migration Utility must identify the relationships by Relationship Template name and Relationship Template Link name.

What You Must Do: Before you run the Migration Utility, change the modified names in Relationship Template or Relationship Template Link to the values in the original Release 11.3.4.

User Interface Changes

In CA APM Release 11.3.4, relationships and links are displayed and modified in separate sections in the user interface. In Release 12.9, relationships and links are combined into a single entity that is displayed and modified in the same section in the user interface.

Some of the menu items for relationship names in Release 12.9 are different from Release 11.3.4. The following chart lists each Release 11.3.4 relationship and its associated Release 12.9 relationship menu item. Some relationship menu items have a different label when viewing the relationship from the reverse direction. For example, the Company Entitlement relationship is displayed as Company Allocation when viewed from the software asset and Software Allocation when viewed from the company.

Release 11.3.4 Relationship	Release 12.9 Entity	Release 12.9 Relationship
Asset Entitlement	Asset (software)	Asset Allocation
Asset Entitlement	Asset (hardware)	Software Allocation
Company Acquisition	Company	Company Acquisition
Company Entitlement	Asset (software)	Company Allocation
Company Entitlement	Company	Software Allocation
Contact Entitlement	Asset (software)	Contact Allocation
Contact Entitlement	Contact	Software Allocation
Governing Document	Legal Document	Governing Legal Document
Image Partitions	Asset	Image Partitions
Legal Amendment	Legal Document	Legal Amendment
Location Entitlement	Asset (software)	Location Allocation
Location Entitlement	Location	Software Allocation
HW Asset Configuration (Generic component)	Asset	Model Configuration
HW Asset Configuration (Specific component)	Asset	Asset Configuration
HW Model Configuration	Model	Model Configuration

Start the CA APM Migration Toolkit

During the upgrade of Release 11.3.4 to Release 12.9, the CA APM Migration Toolkit is installed on the same computer that is performing the upgrade. We recommend that you migrate your CA MDB data to the new release data structures immediately after the upgrade is complete.

Start the CA APM Migration Toolkit on the same computer where you performed the upgrade.

Follow these steps:

- Click Start, All Programs, CA, Asset Portfolio Management, CA APM Migration Toolkit.

Run the Pre-Migration Reports

Before you migrate the CA MDB, you run the pre-migration reports. The pre-migration reports identify the following types of data:

- Data that can cause problems during data migration. You correct the data in the CA MDB *before* you run the Migration Utility (see page 57). For example, if you renamed a relationship template that was provided with Release 11.3.4, this change could cause a problem during the migration of relationships. The Relationship Report identifies the renamed templates, which you change back to the original product-provided template names, before migration.
- Data that requires analysis for migration configuration decisions.
- Data that is not migrated with the Migration Utility, but can be migrated manually with updated product features. You reference this data during manual migration (see page 69), *after* you run the Migration Utility. You must capture the data in these reports before you migrate your legacy data, because this data is not migrated to the Release 12.9 database structures. You save these reports and reference their information later, during manual migration (see page 69) for Release 12.9.
- Data that is supported in Release 11.3.4 but is not supported in Release 12.9. You cannot migrate this data with the Migration Utility or add it using Release 12.9. These reports identify unsupported data and provide legacy reference information.

Note: For information about the features that are supported in Release 12.9, see the CA IT Asset Manager Product Roadmap and the Differences Between CA IT Asset Manager 12.9 and Prior Releases (CA IT Asset Manager 12 and CA Asset Portfolio Management 11.3.4) documents on the CA Support website.

Follow these steps:

1. On the CA APM Migration Toolkit main window, click Migration Reporting.

   The following Pre-Migration Reports area check boxes are selected:

   - Custom Index
   - Duplicate Asset Name
   - Reconciliation
   - Relationships

   Note: If you do not want to generate all reports, select only those report types that you want.

2. In the Report Output Folder area, click Browse and select the output folder where you want to save the reports.
3. Click Generate Reports.

   The status messages appear in the Messages area to help you monitor the report generation process.

   You are prompted to open the report output folder to view the reports.
4. Click Yes.

   Windows Explorer opens. The Reporting tool creates a folder for each report check box that you selected previously.
5. Navigate to, and open, a report folder.

   The reports appear in comma-separated value (CSV) format.
6. Right-click a report and select Open with, Excel, to open and view the report in a table format.

   The report data (see page 49) is presented in a table format. The table headings are in the first row.

   Note: You can click open the report to view in a text editor in CSV format.

Pre-Migration Report Data for Reference and Corrective Action

The Reporting tool generates reports in CSV format that you can open with a text editor. The report field names and field values are separated with commas. You can also open a report with Excel, which presents the data in a table format. When you open a report with Excel, the field names are the column headings, and the field values appear in the rows below the headings.

The following pre-migration reports give you information about data that you must change in the CA MDB *before* migration. The related objects can then be migrated successfully to the Release 12.9 CA MDB data structures.

- Custom Index Report (see page 50)
- Relationship Report (see page 51)

The following reports identify data that you analyze for migration configuration decisions:

- Duplicate Asset Name Report (see page 53)
- Reconciliation Report:
  - Main Translation List Query Report (see page 54)

The following pre-migration reports identify data that you use *after* you run the Migration Utility (see page 57), when you perform manual migrations (see page 69). Save these reports and reference them during manual migration.

- Reconciliation Reports:
  - Main Task Query Report (see page 54)
  - Task Add Asset Report (see page 54)
  - Customized Search Report (see page 55)

The following reports identify data that is not supported in Release 12.9 and that provide legacy reference information:

- Reconciliation Reports:
  - Translation List Obsolete Report (see page 55)
  - Translation List Unconverted Report (see page 55)

Custom Index Report

The Custom Index Report identifies indexes that were added to fields in Release 11.3.4 (or previous releases) for customization. These indexes can create performance issues in Release 12.9. We recommend that you remove custom indexes from your database (see page 50). The report provides SQL statements that you run to remove the custom indexes.

Remove Custom Indexes from Database

We recommend that you remove custom indexes from your database to avoid performance issues. Remove the indexes *before* you run the Migration Utility. The Custom Index Report (see page 50) provides the information that you use to remove the custom indexes.

Follow these steps:

1. Locate the Custom Index Report.
2. Copy the SQL statements from the Drop SQL column on the report.

   Note: Delete the quotation marks at the beginning and end of the statements.
3. Paste the SQL statements to your preferred tool, for example, Microsoft SQL Server Management Studio and Oracle SQL Developer, and run the statements.

   The following items are removed:

   - Custom indexes
   - Index definitions from the arg_index_member table
   - Index information from the arg_index_def table

Relationship Report

The Relationship Report identifies the relationship templates that were renamed from the original product-provided Release 11.3.4 names. Change this data in the CA MDB *before* migration.

The tool generates the Relationship Report in different languages. Use the appropriate report for the language that the Release 11.3.4 was configured to.

The report shows the following status for the relationship template or the relationship template link:

Customized

Indicates that the relationship templates or relationship template links are added or renamed by the user in Release 11.3.4.

- If the relationship was added in Release 11.3.4, it is not a product-provided relationship in Release 12.9. However, it is migrated to a custom relationship.
- If the relationship is product provided in Release 11.3.4 and in Release 12.9, you can migrate the relationship to the product-provided relationship in Release 12.9. First, rename the relationship templates or relationship template links to their original values.

Migrated by Migration Utility

Indicates that the relationship templates or the relationship template links are supported in Release 12.9 and will be migrated by the utility.

No Longer Supported

Indicates the relationship templates or relationship template links that are not product provided in Release 12.9. The Migration Utility migrates these relationships to custom relationships.

Not Found

Indicates the product-provided relationship templates or relationship template links in Release 11.3.4 that are not found in the database of the user. If the relationship templates or relationship template links were renamed and are product provided in Release 12.9, rename the relationship templates or relationship template links to their original values to migrate the relationship to Release 12.9.

Rename to migrate

Indicates the renamed relationship templates or relationship template links in Release 11.3.4 that you have to change to the original name before migrating.

Complete the following actions if you want to include the renamed product-provided Relationship Templates in the migration:

- Change the renamed Relationship Template to the original product-provided name (see page 52).
- Change the renamed Relationship Template Link to the original product-provided name (see page 53).

Change the Renamed Relationship Template to the Original Product-Provided Name

Before you run the Migration Utility (see page 57), you change the renamed Relationship Template names to the original product-provided Relationship Template names from Release 11.3.4.

You execute a SQL statement to change the Relationship Template Name. Perform these steps for each entry in the report with status 'Rename to migrate' and a value that is specified under 'Relationship Template Rename'.

Follow these steps:

1. Execute the following SQL statement from your preferred tool (for example, Microsoft SQL Server Management Studio or Oracle SQL Developer):

   Note: The brackets and the text within the brackets are placeholders. The placeholder names represent the column names on the Relationship Report.

```
UPDATE arg_actiondf
SET adtext = '{Relationship Template Rename}'
WHERE adtext = '{Relationship Template Name}'
    AND ad1obty IN (SELECT slentry
            FROM arg_strlst
            WHERE slid = 9
            AND slvalue1 = '{Relationship Object Type}')
```

2. Replace the placeholders with the values in the same-named columns on the Relationship Report. For example, the report Relationship Template Rename column identifies the product-provided name Activity Summary. You replace {Relationship Template Rename} with Activity Summary.

Change the Renamed Relationship Template Link to the Original Product-Provided Name

Before you run the Migration Utility (see page 57), you change the renamed Relationship Template Link Names to the original product-provided Relationship Template Link Names from Release 11.3.4.

You execute a SQL statement to change the Relationship Template Link Name. Perform these steps for each entry in the report with status 'Rename to migrate' and a value that is specified under 'Link Rename'.

Follow these steps:

1. Execute the following SQL statement from your preferred tool (for example, Microsoft SQL Server Management Studio or Oracle SQL Developer):

   Note: The brackets and the text within the brackets are placeholders. The placeholder names represent the column names on the Relationship Report.

   ```
   UPDATE arg_linkdef
   SET ndtext = '{Link Rename}'
   WHERE ndtext = '{Link Name}'
       AND nd2obty IN (SELECT slentry
               FROM arg_strlst
               WHERE slid = 9
               AND slvalue1 = '{Link Object Type}')
   ```

2. Replace the placeholders with the values in the same-named columns on the Relationship Report. For example, in the report, the Link Rename column identifies the product-provided template link name as Approved by. You replace {Link Rename} with Approved by.

Duplicate Asset Rename Report

The Duplicate Asset Name Report identifies non-unique asset names.

Note: Only the assets that share the same asset name and have no values set for the following registration fields are affected:

- Serial Number
- Alt Asset ID
- Host Name
- DNS Name
- Mac Address
- Serial Number

During migration, the CA APM Migration Toolkit can automatically configure a unique Asset Name for each duplicate Asset Name in your CA MDB. Use the Duplicate Asset Name Report to help you decide how to specify the asset rename configuration (see page 55).

Reconciliation Reports

The Reporting tool generates the following reconciliation reports:

- Main Translation List Query Report (see page 54)
- Translation List Obsolete Report (see page 55)
- Translation List Unconverted Report (see page 55)
- Main Task Query Report (see page 54)
- Task Add Asset Report (see page 54)
- Customized Search Report (see page 55)

Main Translation List Query Report

The Main Translation List Query Report identifies legacy translation list data for companies, operating systems, and models. You analyze the data on this report to determine whether to use the Migration Utility to migrate legacy translation lists to the corresponding Release 12.9 normalization rules or migrate the lists manually.

If you decide to migrate the translation lists manually (see page 83), use the data on the Main Translation List Query Report.

Main Task Query Report

The pre-migration Main Task Query Report identifies data that you use *after* you run the Migration Utility (see page 57). The report provides information about the legacy reconciliation tasks from Release 11.3.4. Save the report and reference it during manual migration of Hardware Reconciliation tasks (see page 82) to create reconciliation rules in Release 12.9.

Task Add Asset Report

The Task Add Asset Report provides data that you use *after* you run the Migration Utility (see page 57), when you perform manual migrations. The report identifies the legacy reconciliation tasks that add owned assets from Release 11.3.4. Save the report and reference it during manual migration of Hardware Reconciliation tasks (see page 82).

Customized Search Report

The Customized Search Report provides data that you use *after* you run the Migration Utility (see page 57), when you perform manual migrations. The report identifies the legacy hardware reconciliation customized searches from Release 11.3.4. Release 12.9 provides predefined hardware reconciliation reports. You can customize these reports using the CA Business Intelligence, which is also provided in Release 12.9. Save the report and reference it during manual migration of hardware reconciliation searches (see page 84).

Translation List Obsolete Report

The Translation List Obsolete Report identifies the Hardware Reconciliation legacy translation lists from Release 11.3.4 that are obsolete and not supported in Release 12.9. This report is for your reference. No action is required.

Translation List Unconverted Report

The Translation List Unconverted Report identifies the Hardware Reconciliation legacy translation lists from Release 11.3.4 that have missing or invalid entries that will not be migrated to Release 12.9. The translation list will be migrated, but some of the entries in the list will not be migrated, because supporting data is not present in the legacy database.

Use the data on the Translation List Unconverted Report and on the Main Translation List Query Report (see page 54) to add the missing entries to the normalization lists (see page 83) after migration.

Specify the Asset Rename Configuration

In Release 12.9, registration includes asset name, serial number alt asset ID, host name, DNS name, and mac address. A *unique* asset name is required for each asset object. Release 11.3.4 did not have this requirement, so your CA MDB could have asset names that are not unique for asset registration. The CA APM Migration Toolkit can automatically configure a unique asset name for each duplicate asset name in your CA MDB during migration.

The CA APM Migration Toolkit uses a configuration to rename the duplicate asset names. You choose the configuration on the CA APM Migration Utility Duplicate Asset Name Configuration dialog. When you run the Migration Utility, the duplicate assets are renamed in your Release 12.9 database.

Note: A unique asset name is a requirement for asset registration by the Common Registration API (CORA) in Release 12.9. If you do not have CORA enabled, asset registration does not occur. Therefore, you do not have to specify the asset rename configuration.

Follow these steps:

1. Review the Duplicate Asset Name Report (see page 53).
2. On the CA Asset Portfolio Management Migration Toolkit main window, click Duplicate Asset Name Configurator.
3. Select one of the following rename configurations:

   Replacement

   Replaces the duplicate asset names with the value in another field. You select this field in the drop-down list.

   Note: The fields in the drop-down list are the same fields that are the headings on the Duplicate Asset Name Report (see page 53).

   The Incrementation configuration is automatically selected and locked. If the Replacement configuration results in a duplicate asset name, adding Incrementation to the configuration ensures that the rename is unique.

   Concatenation

   Appends the values of one or more fields onto the end of the duplicate asset names. You select up to four fields in the drop-down lists.

   Note: The fields in the drop-down lists are the same fields that are the headings on the Duplicate Asset Name Report (see page 53).

   The Incrementation configuration is automatically selected and locked. If the Concatenation configuration results in a duplicate asset name, adding Incrementation to the configuration ensures that the rename is unique.

   Incrementation

   Appends a unique integer value to the end of the duplicate asset names and increments the integer by one for each subsequent duplicate asset name. You enter the starting integer in the Integer Base Line Value.

   NONE

   Duplicate asset names are not renamed. You can select this option if you do not have CORA enabled or if you want to correct the assets manually after migration.

4. (Optional) Enter a one-character Field Delimiter that appears between each field and between a field and an incrementation integer in the Incrementation and Concatenation configurations.
5. Click Save.

   Note: Depending on the number of records, it takes some time for the configuration to save. The progress bar indicates the status of completion.
6. Click Exit.

Run the Migration Utility

The Migration Utility migrates audits, objects, and events from one CA APM release to the upgraded database structure of another.

The hierarchical structure of the objects in the selection area on the CA APM Migration Utility window allows you to select all objects within a hierarchy level or to select individual objects within a level. A status icon displays the migration status for each object or object level.

The icon key in the top area of the window indicates the statuses. When an object status is Complete, you cannot select the object.

The Messages and Summary tabs allow you to monitor the migration process (see page 62) and to review the migration run.

Important: In addition to the services and the scheduled tasks detailed in Prerequisites (see page 43), ensure the Release 12.9 services are not running before you run the Migration Utility.

The first time that you open the window, you are prompted to confirm the migration database versions (see page 59). After you complete this task, you can run the object migrations (see page 60).

Important! With Release 12.9, you can migrate objects that were not migrated with Release 12.8. These objects are costs and payments extensions and audits, custom relationships and audits, and relationship extensions and audits. With this release, all relationships are migrated, including custom relationships and relationships that were not product-provided. If you previously migrated your data from Release 11.3.4, you can migrate the data for just these objects. You do not need to perform the complete data migration again.

You can migrate the following objects and associated events with the Migration Utility:

- Assets
  - Unique Asset Names for CORA
  - Asset Current Status History

- Cost and Payments
  - Billing Codes
  - Pricing Types
  - Cost Types
  - Currency Types
- Cost and Payment Extensions (and the associated audits)
- Legal Documents
  - Legal Definitions
  - Document Locations
  - Legal Status
  - Legal Document Status Histories
- Notes
  - Note Types
- OOTB Relationships (Original Product-Provided Relationships)
- Custom Relationships (and the associated audits)
- Extensions
  - Simple Extensions
  - List Extensions
  - Location Hierarchies
- Relationship Extensions (and the associated audits)
- Attachments
- Roles
- Reconciliation Translation Lists (supported types only)
  - Operating System Translation List
  - System Model Translation List
  - Manufacturer Translation List
- Legacy audits to audit archive tables. The Audit History object is enabled after you migrate other objects and the Audit Generation for Events shows the status as Complete.

Note: To ensure that events work properly in the product, select Audit Generation for Events from the list of Migration Objects. Audit Generation for Events establishes baseline audit records.

Confirm the Migration Database Versions

You confirm the migration database versions by testing the database connection. The first time that you run the Migration Utility, the CA APM Migration Utility Configuration dialog automatically opens. The dialog fields are populated with the database configuration settings that you specified during the Release 12.9 installation.

Note: After you confirm the migration database versions, click Configure on the Migration Utility window.

When you test the database connections, the Migration Utility detects the product release version *from* which you are migrating data and the release version *to* which you are migrating data. The utility populates the From Version and To Version fields on the dialog with the detected product release versions. You cannot change the release versions on the dialog.

The detected From Version must be Release 11.3.4 and the detected To Version must be Release 12.9. If the Migration Utility detects a different release version, you cannot proceed with the migration.

Follow these steps:

1. Enter the Database Password.
2. Click Test Connection.

   A confirmation message indicates that the connection test succeeded or failed.
3. Click Save on the CA APM Migration Utility Configuration dialog if the confirmation message indicated that connection testing succeeded.

   The dialog closes.
4. If the confirmation message indicated that the database connection test failed, determine why the Migration Utility could not connect to the database configuration. After you resolve the problem, repeat the connection test.

   Note: If the Product Release Versions on the CA APM Migration Utility Configuration dialog do not match the release versions that you are trying to connect to the Migration Utility, the database connection test fails. You cannot proceed with the migration.

If you want to change the database configuration settings later, see Configure the Migration Database (see page 60).

Configure the Migration Database

You do not need to configure the migration database during the migration. The database is configured to the settings that were specified during the Release 12.9 installation.

Later, if you change the location of the CA MDB, configure the migration database to the new location before you run the Migration Utility.

Follow these steps:

1. Click Configure on the Migration Utility window.
2. Enter the configuration settings.
3. Click Test Connection.

   A confirmation message indicates that the connection test succeeded or failed.
4. Click Save on the CA APM Migration Utility Configuration dialog if the confirmation message indicated that the connection test succeeded.

   The CA APM Migration Utility Configuration dialog closes.
5. If the confirmation message indicated that the database connection test failed, determine why the Migration Utility could not connect to the database configuration. After you resolve the problem, repeat the connection test.

Run the Object Migrations

Important: In addition to the services and scheduled tasks detailed in Prerequisites (see page 43), ensure the Release 12.9 services are not running before you run the Migration Utility.

The CA APM Migration Utility window lists the migration objects in a hierarchical structure in the CA APM Objects area. You select the objects that you want to migrate. You can migrate the data in stages. The hierarchical structure allows you to select all objects within a hierarchy level or to select individual objects within a level.

When you select an object to migrate, all objects within the hierarchy of that object are also selected. These objects are called secondary objects. The secondary objects within the hierarchy migrate first, and the top-level object that you selected migrates last. For example, if you select the Cost and Payments top-level object, the Billing Code, Pricing Type, and Cost Type secondary objects within the Cost and Payments object hierarchy are also selected. Expand the top-level object to see its secondary objects. During migration, Billing Code, Pricing Type, and Cost Type migrate first. The top-level object Cost and Payments migrates after its secondary objects.

You can clear the check boxes next to the objects that you do not want to migrate. You can select one object, a group of objects, or all objects to migrate.

Objects that have already been migrated have a status of Completed, and their check boxes are disabled. In this way, the Migration Utility prevents you from trying to migrate an object that has already been migrated.

Right-click an object to view options that you can select to perform. The options that are available depend on the status of the object. The following options are available for you to select when you right-click an object:

- Clear the check boxes for the secondary objects
- Move to Completed
- Moved to Not Started

The Audit History object is disabled initially. You start with migrating the non-audit objects. The audit history object is enabled when the migration is successful and the Audit Generation of Events shows the status as Complete. You can migrate the Audit History objects anytime once the option is enabled, and all the applications and services are back online.

Important! Depending on the size of the data, Audit History objects can take a long time to migrate. If the audit history has approximately 1 million records, it is recommended to migrate it during off peak hours.

Follow these steps:

1. On the CA APM Migration Utility window, select the check boxes next to the objects that you want to migrate.

   Note: To ensure the events work properly in the product, select Audit Generation for Events from the list of Migration Objects. Audit Generation for Events establishes baseline audit records.

2. Click Start.

   Look at the information in the Messages tab to monitor the migration progress (see page 62).

   When the migration is successful, the objects in the selection area of the window have a status of Completed.

   Note: If the migration fails, view the details in the object migration log files in the following location:

   [ITAM Root Path]\Migration Toolkit\migration-utility\logs

3. (Optional) If the migration is successful, select the Audit History object and repeat Step 2.

4. Click Exit.

   The CA APM Migration Utility window closes.

When the migration completes, restart the services for the following Service Management products:

- CA Service Catalog
- CA Service Desk Manager
- CA Client Automation
- CA APM Release 12.9

Monitor the Migration Process

The Messages tab on the CA APM Migration Utility window shows the progress of the current migration process. You monitor the migration process by viewing the messages. The messages indicate the changing status of each object that is being migrated.

When the migration is finished, you can view a summary of the successful, pending, and failed migrations on the Summary tab. The Summary tab shows the migration status for all migrations that ran during your session.

You can view the object migration log files from the following location:

[ITAM Root Path]\Migration Toolkit\migration-utility\logs

For any failure messages appearing in the log files, contact CA Support.

Run the Post-Migration Reports for Manual Migrations

After you run the Migration Utility, run the post-migration reports, which you use during manual migrations. The post-migration reports identify object data that you have to enter into Release 12.9. The utility could not migrate some data because the feature associated with the data changed.

Follow these steps:

1. On the CA APM Migration Toolkit main window, click Migration Reporting.
2. Clear all of the check boxes in the Pre-Migration Reports area and select the following reports in the Post-Migration Reports area:
   - Advanced Searches
   - Attachments
   - Basic Search Return Fields
   - Events
   - Filters
   - Role Security (Field and Functional Permissions)

   Note: If you do not want to generate all post-migration report types, select only those report types that you want.
3. In the Report Output Folder area, click Browse, and select the output folder where you want to save the reports.
4. Click Generate Reports.

   The status messages appear in the Messages area to help you monitor the report generation process.

   You are prompted to open the report output folder to view the reports.
5. Click Yes.

   Windows Explorer opens. The Reporting tool creates a folder for each Post-Migration Reports check box that you selected previously.
6. Navigate to, and open, a report folder.

   The reports appear in comma-separated value (CSV) format.
7. Right-click a report and select Open with, Excel, to open and view the report in a table format.

   The report data (see page 64) is presented in a table format. The table headings are in the first row.

   Note: You can open a report and view in a text editor, in CSV format.

Migration Report Data for Reference and Analysis

The Reporting tool generates reports in CSV format that you can open with a text editor. The report field names and field values are separated with commas. You can also open a report with Excel, which presents the data in a table format. When you open a report with Excel, the field names are the column headings, and the field values appear in the rows below the headings.

The post-migration reports give you information about data that you enter in Release 12.9 *after* migration. This data could not be migrated using the Migration Utility.

The following post-migration reports provide information that you use to perform manual migrations (see page 69):

- Advanced Search Report (see page 64)
- Attachments Report (see page 65)
- Basic Search Report (see page 66)
- Event Reports (see page 66)
- Filtering Reports (see page 67)
- Role Security (Field and Functional Permissions) Reports (see page 68)

Advanced Search Report

The Advanced Search Report provides a summary of each advanced search and location information for the detail reports for each advanced search (see page 65). The Detail column of the report provides the location and name of each Advanced Search Detail Report.

The following report fields require an explanation:

Export Type

Indicates the Export Format for search results.

Refresh Interval

Identifies the start time and frequency for an Export Schedule.

Object Type

Indicates Role Access when the Security Search setting has one or more roles.

Assignment

Identifies the role name or contact that has permission to access the search.

Creator

Identifies the name of the last user to update the search. Use this information to delegate the manual migration (re-creation) of the advanced search. You do not assign this field to a setting in the advanced search.

Creator ID

Identifies the name of the last user to update the search. Use this information to delegate the manual migration (re-creation) of the advanced search. You do not assign this field to a setting in the advanced search.

Use the Advanced Search Report to migrate the advanced searches to Release 12.9 manually (see page 72).

Advanced Search Detail Reports

Each Advanced Search Detail Report identifies the data for one advanced search. Review the information about advanced searches that were created in Release 11.3.4.

Use the Advanced Search Detail Reports to migrate these advanced searches to Release 12.9 manually (see page 72).

Attachments Report

The Attachments Report identifies information that you use to migrate file attachments manually (see page 76). The Migration Utility migrates the complete Web URL link attachments and the metadata for remote server and local file attachments. After migration, you move the physical file attachments to the Storage Manager Service.

The Attachments Report provides the file location and description and the following information for each attachment:

UUID

Universally Unique Identifier identifies an object and distinguishes between two objects that have the same name.

Object Type

Identifies the type of object to which the file is attached.

Assignment

Identifies the name of the object to which the file is attached.

Basic Search Report

Use the Basic Search Report to view the following information about searches that were created in Release 11.3.4 and to migrate these basic searches to Release 12.9 manually (see page 70):

- Object Type that the search returns.
- Role, if any, permitted to view the search return fields.
- Search Return Fields, which were named Display Fields in Release 11.3.4.

Event Reports

The Notification History Event Report (see page 66) provides history information from Release 11.3.4, for you to review. The following Event Reports identify data that you use *after* you run the Migration Utility (see page 57), when you perform manual migrations. Reference these reports during manual migration of events (see page 77):

- Date Event Report (see page 67)
- Watch and Change Event Report (see page 67)

Notification History Event Report

The Notification History Event Report provides history information from Release 11.3.4 for you to review. No action is required.

This report identifies events that were processed in the last year. The following fields require explanation:

Event Enabled

Indicates that the event is enabled and not inactive when the value is TRUE. Indicates that the event is inactive when the value is FALSE.

Event Field Name

The event is based on the value of this object field.

Event Recipient

The email address of the current event notification.

Event Notification Definition Text

The email message text of the current event notification.

Notification Type

Indicates the type of notification that the recipient receives. "Initial Event" indicates the recipient of the first notification. "Escalation" indicates the recipient of unacknowledged notifications.

Notification Text

The email message text of the past event notification.

Notification Recipient

The email address of the past event notification.

The *Implementation Guide* provides information about workflow provider process parameters that are specified in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Date Event Report

The Date Event Report identifies data that you use *after* you run the Migration Utility (see page 57), when you perform manual migrations. This report identifies date events and notifications. Reference the report during manual migration of events (see page 77).

The Implementation Guide provides information about workflow provider process parameters that are specified in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Watch and Change Event Report

The Watch and Change Event Report identifies data that you use *after* you run the Migration Utility (see page 57), when you perform manual migrations. This report provides information about watch events and notifications and about change events and notifications, from Release 11.3.4. Reference the report during manual migration (see page 69).

Note: Manual events were available in Release 11.3.4, but are not supported in Release 12.9. Manual events are not included on the Watch and Change Event Report.

The Implementation Guide provides information about workflow provider process parameters that are specified in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Filtering Reports

The Filtering Report provides a summary of each filter and location information for the detail reports for each filter (see page 67). The Detail column of the report provides the location and name of each Filter Detail Report.

Contact Filtering Detail Report

Each Filtering Detail Report identifies the data for one filter. Use the Filtering Detail Reports to view the information about filters that were created in Release 11.3.4 and to migrate filters manually (see page 78).

Role Security (Field and Functional Permissions) Reports

Each Role Security Report identifies the data for one field, functional, or viewable linked object security setting. The Migration Toolkit generates the following types of role security reports:

- **Field Security Reports.** Generates one Field Security Report for each object that has role security settings. The report identifies the role, the object, the object field, and the permission that is assigned to the role for the field. The Update Permission report column label and the Add New Permission report column label refer to Release 11.3.4 functionality. Release 12.9 does not differentiate permissions for updating and creating objects.
- **Functional Security Reports.** Generates one Functional Security Report for each object that has role security settings. The report identifies the role, the object, the function related to the object, and the permission that is assigned to the role for the function.
- **Field Security Linked Object Viewable Report.** Generates one Field Security Linked Object Viewable Report for each object that has role security settings. The report identifies the role, the objects, and the assigned fields for the object.

Use the Role Security Reports to view the information about role security settings that were created in CA APM Release 11.3.4 and to migrate role security settings manually (see page 79).

The following objects, fields, and functions are not supported in Release 12.9. They appear on the Release 11.3.4 database reports for reference only:

- Asset Version
- Asset Version Status History
- Model Version
- Keywords

Start CA APM Web Interface

You start the CA APM web interface to run the Release 12.9 upgraded product and manually migrate data to the Release 12.9 database. Complete the Migration Utility (see page 57) automated migrations and run the post-migration reports (see page 63) *before* you perform manual migrations (see page 69).

To start the web interface, open a web browser and enter the following URL:
`http://servername/itam`

Replace *servername* with the name of the server that is hosting the CA APM web servers.

Note: If the Internet Explorer browser security is set to high, a content warning message appears when you start the web interface. To avoid this message, add the web site to your trusted sites or lower your security settings.

A Start menu shortcut is created on your web server that references the URL location.

To log in to CA APM after you open the URL, enter the following default credentials:

User Name

uapmadmin

Password

uapmadmin

Note: In some situations, a browser error or a user name error appears. You can resolve these errors by following the troubleshooting instructions (see page 86).

Perform Manual Migrations

You can perform the manual migration of data to Release 12.9 after you complete the following tasks:

- You migrated data using the Migration Utility.
- You generated the post-migration reports.

When you migrate data manually, you use Release 12.9 to enter the data in the new-release data structures. The migration reports specify the fields and values that you enter.

Important: Exit the Migration Toolkit and start the web interface (see page 68) before you can perform the manual data migrations.

Perform the following manual migrations:

- Migrate Basic Searches (see page 70)
- Migrate Advanced Searches (see page 72)
- Migrate File Attachments (see page 76)
- Migrate Events (see page 77)
- Migrate Filters (see page 78)

- Migrate Role Security (Field and Functional Permissions) (see page 79)
- Migrate Hardware Reconciliation Tasks and Rules (see page 82)
- Migrate Hardware Reconciliation Translation Lists (see page 83)
- Migrate Hardware Reconciliation Searches (see page 84)

Migrate Basic Searches

In Release 11.3.4, the search return fields that a user can see are set in the Security feature by role. Release 12.9 enhances the Basic Search functionality so that it is more closely aligned to the Advanced Search. All fields are available in the Basic Search. In Release 12.9, you set the search return fields that a user can view in the search feature. When you create a search and save the configured search, you can apply security to the search by selecting specific user roles and configurations.

By default, the security for the searches you create makes them available only to the creator. You assign roles and configurations to your searches to grant access to the users who are assigned to those roles and configurations.

Note: For information about searching, see the *User Guide*.

These changes cannot be migrated with the Migration Utility. Use the Basic Search Report data during the manual migration.

Follow these steps:

1. Identify the Object Type for the search on the Basic Search Report.
2. In CA APM, click the tab and optional subtab for the object that you want to find.
3. On the left, click New Search.

   The Add Fields dialog appears.

   Note: For some object types, you are prompted to select templates, families, or other attributes to narrow the search.
4. Using the report Search Return Fields, select the fields to add to the search. In Release 11.3.4, these fields were labeled Display Fields.
5. In the Add Fields(s) To area at the bottom of the dialog, select Search Criteria and Search Results.
6. Click OK.

   The fields are added to both the search criteria and search results. The Add Fields dialog closes.

7. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.

8. In the Search Information area, enter the search title and any other descriptive information, for example, Category and Description.

9. (Optional) Open the Search Security area.

10. (Optional) In the Search Security area, select the user roles for which the search is available.

    Note: We recommend that you select the user role that is identified on the Basic Search Report (see page 66).

11. (Optional) In the Search Security area, select the configuration for which the search is available.

    Note: If you do not select either a role or a configuration, the search is available only to the search creator.

12. Locate the Search Criteria area and the criteria fields that you entered.

13. For each Search Criteria field, enter the field value. You can click the search icon to search for a value.

14. (Optional) Open the Additional Settings area, and add other settings, for example, sorting settings.

15. Click Save.

    The search is saved.

16. If you selected user roles in the Search Security area, perform the following steps for each role:

    a. Click Administration, User/Role Management.

    b. On the left, expand the Role Management menu.

    c. Click Role Search.

    d. Search for and select the role.

       The role details appear.

    e. In the Default Searches area, click Select New.

    f. Search for the search that you just created.

    g. Assign the search as a default search for the role.

    h. Click Save.

       The updated role is saved.

Migrate Advanced Searches

In CA APM Release 11.3.4, the search return fields that a user can see are set in the Security feature by role. In Release 12.9, searches support an added level of security. You set the search return fields that a user can view in the search feature. When you save the configured search, you can apply security to the search by selecting specific user roles and configurations.

By default, the security for the searches you create makes them available only to the creator. You assign roles and configurations to your searches to grant access to the users who are assigned to those roles and configurations.

Note: For information about searching, see the *User Guide*.

These changes cannot be migrated with the Migration Utility.

When you migrate Advanced Searches, you complete the following steps:

- Create the Advanced Search (see page 72)
- Schedule a Search and Export Results (see page 75)

Create an Advanced Search

Use data from the Advanced Search Report (see page 64) and the Advanced Search Detail Report (see page 65) during the manual migration.

Follow these steps:

1. Identify the Object Type for the search on the Advanced Search Detail Report.
2. In CA APM, click the tab and optional subtab for the object that you want to find.
3. On the left, click New Search.

   The Add Fields dialog appears.

   Note: For some object types, you are prompted to select templates, families, or other attributes to narrow the search.
4. On the detail report, identify the fields that are in *both* the Return Fields and the Selected Criteria Fields.
5. On the Add Fields dialog, select the common fields that you identified on the report.

6. In the Add Fields(s) To area at the bottom of the dialog, select Search Criteria and Search Results.
7. Click OK.

   The fields that are both Search Criteria and Search Results fields are added to the search, and the Add Fields dialog closes.
8. Click Add Fields.

   The Add Fields dialog appears.
9. Select the Return Fields that are not common to the Return Fields and the Selected Criteria Fields on the detail report.
10. In the Add Fields(s) To area at the bottom of the dialog, select Search Results Only.
11. Click OK.

    The Search Results Only fields are added to the search, and the Add Fields dialog closes.
12. Click Add Fields.

    The Add Fields dialog appears.
13. Select the Selected Criteria Fields that are not common to the Return Fields and the Selected Criteria Fields on the detail report.
14. In the Add Fields(s) To area at the bottom of the dialog, select Search Criteria Only.
15. Click OK.

    The Search Criteria Only fields are added to the search, and the Add Fields dialog closes.
16. At the top of the page, click CONFIGURE SEARCH: OFF.

    The configuration of the search is complete.
17. In the Search Information area, enter the search title and any other descriptive information from the report. For example, Category and Description.

18. (Optional) Expand the Search Security area.
19. (Optional) In the Search Security area, perform the following steps to select the user roles for which the search is available:
    a. Click Select New in the Role Access area.

       The Role Search dialog opens.
    b. Enter the Role Name that is identified in the Assignment field on the Advanced Search Report. Role Name can be the name of a role or a contact name.
    c. Enter a Description, if you want.
    d. Select whether to include Inactive records in the search for the new role.
    e. Click Go.

       The search results appear.
    f. Select the roles or contacts for which the search is available.
    g. Click OK.

       The Role Search dialog closes.
20. (Optional) In the Search Security area, select the configuration for which the search is available.

    Note: If you do not select either a role or a configuration, the search is available to all users and configurations.
21. Locate the Search Criteria area and the criteria fields that you selected.
22. Click Advanced.

    The advanced Search Criteria area opens.
23. For each Search Criteria, perform the following steps:
    a. Click the Edit Record icon next to a Search Criteria.
    b. Locate the Criteria information about the report.
    c. Enter the Operator, Value, Connector, and parenthesis, as indicated on the detail report.
    d. Click the Complete Record Edit icon.
24. (Optional) Open the Additional Settings area, and add other search settings, for example, sorting.

    Note: In the Search Results Sorting area, select the Selected Field and Sort Direction values, as identified on the detail report Sort Order area.
25. Click Save.

    The advanced search is saved.

Schedule a Search and Export Results

You can schedule a search to process periodically and export the search results to a CSV file or a database view.

Follow these steps:

1. In CA APM, click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.
3. Search for and select the search that you saved.
4. On the left, click New Export.
5. Enter the basic export information that is based on the detail report export information.
6. The following fields require explanation:

   Export name

   Specifies the export name.

   Export Format

   Specifies the format for the exported search results.

   View Name

   Specifies the database view name.

   Note: The view name is required if you select Database View for the Export Format. The name must be a valid database view name.

   Description

   Specifies a description for the exported search results.

   Retention Days

   Specifies the number of days that the exported search results are retained before the results are purged.

   Folder Name

   Specifies the folder for the exported CSV file search results.

   Never Expires

   Specifies that the CSV file or database view is never purged.

7. Schedule the search in the Export Schedule area. Use the detail report Refresh Interval value to schedule the search.

   The following fields require explanation:

   Run Time

   Specifies the time of day to process the search, in the local time zone on the CA APM application server.

   Interval Type

   Specifies the type of interval for the search, for example, Day, Month, Quarter, Week, or Year.

   Interval Day

   Specifies the day during the interval to process the search. For example, if the Interval Type is Month and the Interval Day is 1, the search is processed on the first day of the month.

   First Run Date

   Specifies the date when the first search starts to process.

   Interval

   Specifies how often the search processes, which are based on the selected Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the search processes every two weeks.

   Last Day of Interval

   Specifies that the search processes on the last day of the selected Interval Type.

8. Specify whether all roles and configurations that are assigned to the search receive the exported search results.
9. Click Save.

   The search is saved. The search processes at the scheduled time and the search results are exported.

Migrate Attachments

In Release 12.9, the Storage Manager Service handles all attachment files. You can specify two types of attachments:

- **Web URL link.** Provides direct access to the page specified in the URL. When you add this type of attachment, include the prefix *http://* for the link to work correctly.
- **File path.** Provides direct access to a file. The file opens using the default program for the file type. At the time that you create this attachment type, the file is copied from your file system to the file system on a CA APM server.

  Note: If you add multiple attachments (to one object or to different objects), the name and file path or URL for each attachment must be unique for all objects.

In Release 11.3.4, file attachments were stored in a common share folder.

The Migration Utility migrates the complete Web URL link attachments and the metadata for remote server and local file attachments. The metadata includes the attachment description information and file path location information. The Migration Utility changes the file path location to the Storage Manager Service. After migration, you move the physical file attachments to the Storage Manager Service.

After you run the Migration Utility, you copy the Release 11.3.4 file attachments from the share folder and your local server to the Release 12.9 Storage Manager Service. Web URL link attachments are migrated by the Migration Utility.

Note: For more information about file attachments, see the *User Guide*.

Use the Attachments Report (see page 65) data during the manual migration.

Follow these steps:

1. Navigate to the file attachment location that is identified on the report.
2. Copy and paste the file attachment to the following location on the Storage Manager Service on the application server:
   - *[ITAM Root Path]*\Storage\Common Store\Attachment*attachment.extn*

   Replace *attachment.extn* with the attachment filename and extension.

   Enter the complete path to the file attachment, for example:

   C:\Program Files (x86)\ITAM\Storage\Common Store\Attachment\legaldoc1.docx
3. Repeat these steps for each remote server or local file attachment on the report.

   Note: Files that are not moved to the Storage Manager Machine location are not available in the product.
4. If you deleted an attachment from the remote server or your local machine, but not from CA APM, the Migration Utility migrates the metadata for the attachment. If the report identifies attachments that no longer physically exist, use Release 12.9 to delete the attachment metadata.

Migrate Events

You can use the user interface to define date, change, and watch events. You can set up notifications using hard-coded text and the CA APM object values. For example, you can specify that the subject of a notification include the words "Acknowledgment required for" followed by the value of the CA APM legal document identifier object. When an event occurs, email notifications can be sent to specific recipients. Notifications that are not acknowledged can be escalated.

Use the Date Event Report (see page 67) data and the Watch and Change Event Report (see page 67) data during the manual migration of events and notifications.

Follow these steps:

1. Follow the instructions for creating events and notifications in the *User Guide*.
2. Use the information in the Date Event Report and the Watch and Change Event Report to create the events and notifications.

   Note: The *Implementation Guide* provides information about workflow provider process parameters that you specify in CA Process Automation. For information about notification process parameters, see your workflow provider documentation.

Migrate Filters

In CA APM Release 11.3.4, the filters that a user can see are set in the Security feature, by role. In this release, filters support an added level of security. You set the filters that a user can view in the filters feature. When you configure a filter, you can apply security to the filter by selecting specific user roles and users who have permission to see the filter.

By default, the security for the filters you create makes them available to all roles and users. By applying unique security to your filters, you ensure that certain users cannot view sensitive information in a filter.

These changes cannot be migrated with the Migration Utility. Use the Filter Detail Reports (see page 67) data during the manual migration.

Follow these steps:

1. Identify the object for the filter on the Filtering Detail Report.
2. In CA APM, click the Administration tab and the Filter Management sub tab.
3. Click New Filter.

   The Filter Details page opens.
4. In the Filter Information area, perform the following steps, using the information in the Filtering Detail Report:

   a. Enter the Filter Name and the Object that you want to filter.

   b. (Optional) Enter a Description.

   c. (Optional) Select Assign Filter to All Users, if you want all users to be able to view the filter data. If you want to apply security to the filter, complete the Filter Security area, as described in the following steps.

5. In the Filter Security area, perform one or more of the following actions:
   - To enter roles that can see the filter:
     - Click Select New in the Roles area.

       The Role Search dialog opens.
     - Search for and select the roles that are permitted to see the filter.
     - Click OK.
   - To enter users who can see the filter:
     - Click Select New in the Users area.

       A search dialog opens.
     - Search for and select the users who are permitted to see the filter.
     - Click OK.
6. Click Add Fields.

   The Add Field(s) dialog opens.
7. Select the fields that appear on the report in the Selected Criteria Fields section.
8. Click OK.

   The Add Field(s) dialog closes and the fields that you selected appear in the Filter Criteria area.
9. Using the information in the Criteria area of the detail report, perform the following steps for each Filter Criteria:
   a. Click the Edit Record icon next to a Filter Criteria.
   b. Enter the Operator, Value, Connector, and parenthesis, as indicated on the report.
   c. Click the Complete Record Edit icon.
10. Click Save.

    The filter is saved.

Migrate Role Security

The Migration Utility migrates user roles, but not the role security settings. You migrate the role security (field, functional, and viewable linked object permissions) manually.

A user role is the primary record that controls security and user interface navigation. Each role defines a focused view of the product by exposing only the functionality necessary for users to perform the tasks that are typically assigned to their roles in their business organization. The default role for a user, together with the user interface configuration, determines what the user sees when logging in. A user can belong to only a single role.

You configure user roles to apply functional and field-level repository access rights. You determine and assign the level of access that is required for each role. Role assignment prevents the users from performing unauthorized tasks, such as adding or deleting data.

Field security defines the role permissions for an object field, for example, full control. Functional security defines the role permissions for functions on an object, for example, copy an asset. Viewable Linked Object Security defines the fields for the object.

You create the security permission settings for an object in the object local configurations. Then, you assign one of the object configurations to a role. The field and functional security permissions for a role are determined by the object configurations that are assigned to that role. The object configuration for each role is identified on the Role Security Reports (see page 68) for the object.

You perform the following manual migrations to migrate the role security:

- Migrate Role Field Security (see page 80)
- Migrate Role Functional Security (see page 80)
- Migrate Role Viewable Linked Object Security (see page 81)

Use the information in the Role Security Reports (see page 68) to migrate the role field security, role functional security, and role viewable linked field security manually.

Migrate Role Field Security

Use the information in the Role Security Reports (see page 68) to migrate role field security manually.

Follow these steps:

1. For role field security permissions, on the Field Security Report for the object, locate a field and the role permission for the field.
2. Create and name a local configuration for the object field. The following field security configurations are available:
   - **Full Control.** The field is editable by the role.
   - **Hidden.** Hidden and removed from the user interface for the role.
   - **Read Only.** The field is read only for the role.

   Note: For information about configuring the user interface, see the *Administration Guide*.

Migrate Role Functional Security

Use the information in the Role Security Reports (see page 68) to migrate role functional security manually.

Follow these steps:

1. For role functional security permissions, on the Functional Security Report for the object, locate a function and the role permission for the function.
2. Create and name a local configuration for the object function. Functional security configurations can be one of many functions, for example, allow users to change the asset model. Functional security configurations have a permission of Granted Permission or Denied Permission.

   Note: For information about configuring the user interface, see the *Administration Guide*.
3. Save the object configuration.
4. Click Administration, User/Role Management.
5. On the left, expand the Role Management area.
6. Click Role Search.
7. Search for the role indicated on the Security Report.
8. Click the role name link in the Search Return area.

   The Basic Information area opens.
9. On the left, click Role Configuration.

   The Role Configuration area appears.
10. Click Select New.

    The list of saved configurations appears.
11. Select the object configuration that you want to assign to the role.
12. Click OK.

    The object configuration is assigned to the role.

Migrate Role Viewable Linked Object Security

Use the information in the Role Security Reports (see page 68) to migrate role viewable linked object security manually.

Follow these steps:

1. For role viewable linked object security permissions, on the Field Security Linked Object Viewable Report, locate a linked object and the role for the object.
2. Create and name a local configuration for the object. Link the fields that are defined as Assigned Fields for the Object in the report.
3. Save the object configuration.
4. Click Administration, User/Role Management.
5. On the left, expand the Role Management area.
6. Click Role Search.
7. Search for the role indicated on the Security Report.
8. Click the role name link in the Search Return area.

   The Basic Information area opens.
9. On the left, click Role Configuration.
10. Click Select New.
11. Select the object configuration that you want to assign to the role and click OK.

The object configuration is assigned to the role. Repeat the steps for each role in the report.

Migrate Hardware Reconciliation Tasks and Rules

The hardware reconciliation process involves the following steps:

1. Establish data normalization rules to map data values between discovery repositories and the product.
2. Define a reconciliation rule to specify how to limit the data being processed and how to process the records that were found.

   Note: The reconciliation rules in this step replace the Release 11.3.4 reconciliation tasks. You create reconciliation rules that are based on the Release 11.3.4 tasks from the Main Task Query Report (see page 54) and the Task Add Asset Report (see page 54), during the manual migration.
3. (Optional) Define reconciliation update options to specify the owned-asset fields that you want the Hardware Reconciliation Engine to update automatically with changes found in the corresponding discovered assets.
4. Define asset matching criteria to match owned and discovered assets for a reconciliation rule.
5. View the reconciliation results in the message queue.

Use the Main Task Query Report (see page 54) and Task Add Asset Report (see page 54) data during the manual migration of tasks to reconciliation rules.

Follow these steps:

1. Follow the instructions for defining reconciliation rules in the Define a Reconciliation Rule section of the *Administration Guide*.
2. Use the information in the Main Task Query Report and Task Add Asset Report to create the reconciliation rules.

Migrate Hardware Reconciliation Translation Lists

If you choose *not* to migrate the Hardware Reconciliation translation lists using the Migration Utility, you migrate the lists manually. You analyze the Main Translation List Query Report (see page 54) to make this decision.

Release 12.9 replaces multiple translation lists of the same type with normalization rules for Model, Manufacturer, and Operating System.

Use the Main Translation List Query Report (see page 54) data during the manual migration of translation lists to normalization rules.

Follow these steps:

1. Follow the instructions for creating normalization rules in the Data Normalization section of the *Administration Guide*.
2. Use the information in the Main Translation List Query Report to create the normalization rules.

   Note: Merge all of the lists of the same type, eliminate duplicate entries, and migrate the combined list to the corresponding normalization rules.

Migrate Missing Entries from Hardware Reconciliation Translation Lists

The Translation List Unconverted Report identifies the Hardware Reconciliation legacy translation lists from CA APM Release 11.3.4 that have missing or invalid entries that are not migrated to Release 12.9. The translation list is migrated, but some of the entries in the list are not migrated, because supporting data is not present in the legacy database.

The product replaces multiple translation lists of the same type with normalization rules for Model, Manufacturer, and Operating System.

Use data from the Translation List Unconverted Report (see page 55) and the Main Translation List Query Report (see page 54) to add missing entries on the legacy translation lists to Release 12.9 normalization rules.

Follow these steps:

1. Follow the instructions for updating normalization rules in the Data Normalization section of the *Administration Guide*.
2. Use the information in the Translation List Unconverted Report (see page 55) to update the normalization rules in Release 12.9 with the missing entries identified in the report.

   Note: Merge all of the lists of the same type, eliminate duplicate entries, and migrate the combined list to the corresponding normalization rules.

Migrate Hardware Reconciliation Searches

You migrate the hardware reconciliation custom searches from CA APM Release 11.3.4 to Release 12.9 hardware reconciliation reports. The product provides predefined hardware reconciliation reports that are generated by CA Business Intelligence software. You can customize these reports using CA Business Intelligence, which is also provided.

Hardware reconciliation reports provide the following information:

- Owned assets that have been reconciled to a discovered asset, including both discovered inventory and network discovery records.
- Billed assets (an active or received asset having a valid bill code) not matched to a discovery record.
- Discovered assets not reconciled to an owned asset.
- Discovered assets not processed due to missing or invalid data.
- Counts of the current discovery data volume.
- Owned assets matched to discovery records.
- Owned assets not matched to discovery records.
- Matches between network discovery data and agent discovery data.
- Potential lost revenue, including assets not being billed, but discovered. This report exposes revenue opportunities that are based on the number of assets being billed. Use the information in this report to provide proof that an asset is active and discovered.
- Network discovery records that have not been matched to a corresponding discovered inventory. Network discovery provides limited data to identify an asset on the network. Discovery provides detailed hardware and software information about an asset.

Use the Release 11.3.4 search information in the Customized Search Report (see page 55) to determine which hardware reconciliation reports to generate and possibly customize.

Follow these steps:

1. Follow the instructions for generating hardware reconciliation reports in the Reporting section of the *User Guide*.
2. Use the information in the Customized Search Report to locate the related hardware reconciliation report and enter the search criteria.

Note: To add unreconciled assets by generating and exporting the results of a report and then importing the report results through Data Importer, follow the instructions in the Add Assets from Unreconciled Discovered Records section of the *Administration Guide*.

Perform Post-Migration Verification

If you had integrations with CA Service Desk Manager and CA Service Catalog before the data migration, perform the post-migration verification of these integrations. You perform this verification after you have completed migrating all data to Release 12.9.

Follow these steps:

1. Click Run and execute services.msc.
2. If the CA Service Desk Manager service is not running, select and start the service.
3. Go to the CA Service Desk Manager directory.
4. If the CA Service Desk Manager PDM Tomcat service is not running, select and start the service.
5. Log in to CA Service Catalog.
6. Go to Administration and click Configuration.
7. Click the CA APM Web Services hyperlink.
8. Click the edit pencil icon for the CA APM web server name.
9. Enter the CA APM web server name.
10. Click the edit pencil icon for the CA APM port number.
11. Enter the port number and click Save.
12. Log out and start the CA Service View service in services.msc.

    Verify that the CA APM integrations with CA Service Desk Manager and CA Service Catalog work.

Troubleshooting

This section contains the following topics:

Web Servers Named with Underscore Characters

Symptom:

Using underscore characters in web server host names cause problems when you log in to the product or when you use CA EEM for user configuration.

Solution:

If you are using a virtual or ghosted system, configure a new host name by creating another image without the underscore character. For a production system, add a host name to your internal Domain Name System (DNS) so that the product can be accessed with a different URL.

Audit History Migration Fails

Symptom:

After you execute the Migration Utility, the status icon for Audit History shows “Error” indicating the migration has failed and the migration utility logs shows the following message:

```
Audit History migration has aborted due to a history data conflict with the Group Separator. Contact CA Support to determine a unique Group Separator.
```

Solution:

Contact CA Support.

Migration Utility Class Error

Symptom:

When you try to launch the Migration Utility from the toolkit or command prompt, you get the following error message:

```
Could not find the main class: com.ca.core.gui.Appplication
```

Solution:

The error occurs if you have configured an incorrect path for the KETTLE_HOME. Ensure that the KETTLE_HOME environment variable is set to the path of Kettle which contains the folder “data-integration”. For example: C:\Program Files\Pentaho\Kettle\.

Duplicate Asset Name Configurator link fails to launch

Valid on Windows 2008 and Windows 7 Operating System

Symptom:

You cannot execute the Duplicate Asset Name Configurator with User Access Control (UAC) turned ON.

Solution:

To execute the Duplicate Asset Name Configurator with UAC turned ON, launch the UI as an administrator.

- Right-click LaunchUI.bat and click Run as Administrator.

Chapter 5: Implementing Multi-Tenancy

This section contains the following topics:

Multi-Tenancy

Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA APM. Tenants only interact with each other in defined ways, as specified by their roles and tenant hierarchies. Typically, unless granted access by a role or tenant hierarchy, each tenant views the CA APM implementation as solely for its own use and cannot update or view the data for another tenant.

Multi-tenancy allows tenants to share hardware and application support resources, which reduces the cost of both, while gaining many benefits of an independent implementation.

Multi-tenancy is installed automatically during the CA APM installation. After you have installed CA APM, follow the steps in this section to implement multi-tenancy.

More information:

How to Implement Multi-Tenancy (see page 92)

Service Provider

The *service provider* is the primary tenant (owner) in a CA APM multi-tenancy implementation. The first tenant added to a CA APM implementation is always the service provider tenant. The service provider tenant cannot have a parent tenant.

CA APM associates the privileged user (typically, uapmadmin) with the service provider tenant.

Only the service provider tenant can perform any of the following CA APM tasks:

- Define, edit, or delete tenants.
- Allow tenants to have subtenants.
- Update tenanted public data.

  Note: The CA APM administrator can grant tenant users access to data other than their own. In addition, a user role can specify separate read and write access to certain tenant groups for users within that role. For more information about creating a user role and assigning a role to a user, see the *Administration Guide*.

How Multi-Tenancy Works

When you enable multi-tenancy (see page 93), you can grant each contact access to all tenants (public), a single tenant, or a tenant group (user-defined or product-maintained). The role for a contact controls access, which specifies read and write access independently.

Note: For more information about creating a user role and assigning a role to a user, see the *Administration Guide*.

If multi-tenancy is enabled, most CA APM objects include a tenant attribute that specifies the tenant that owns the object. Objects are categorized into three groups, depending on their tenant attribute and how the object is used:

Untenanted

Defines objects without a tenant attribute. All data in these objects is public, and any user can create and update untenanted public data.

Tenant Required

Defines objects with a tenant attribute that cannot be null (enforced by CA APM, not the DBMS). All data in these objects is associated with individual tenants; there is no public data.

Tenant Optional

Defines objects with a tenant attribute that can be null. You can either create these objects as tenanted or public. When you select a tenant in a tenant drop-down to create an object, the object becomes a tenanted object. However, when you select the Public Data option in a tenant drop-down, the object becomes a tenanted public object. Users assigned to a role that only exposes a single tenant do not see a tenant drop-down when entering data.

When a user queries the database, the product restricts the results to objects belonging to tenants that the user is authorized to access. As a result, you never see data in tenant required tables except for the data that belongs to tenants that you are permitted to access. If the data is tenanted public data, you can see the data in tenant optional tables because the data is also public data.

When a tenant user asks to create or update a database object, the product verifies that the object belongs to a tenant that the current role for the user can update. The product also verifies that all references from the object to other objects are to public (untenanted) objects, to objects from the same tenant, or to objects from tenants in the tenant hierarchy above the tenant for the object. That is, a tenanted object is allowed to reference objects belonging to its parent tenant, to the parent of the parent, and so on.

If a user who creates an object has update access to multiple tenants, the user must specify the tenant explicitly, either directly or indirectly.

Note: The referenced objects restriction has one exception. Certain references are permitted to reference objects that belong to tenants in the tenant hierarchy of their containing object. These references are designated as SERVICE_PROVIDER_ELIGIBLE in the CA APM object schema. The SERVICE_PROVIDER_ELIGIBLE setting makes a difference only if the service provider tenant is not in the tenant hierarchy above the tenant for the object; if the service provider tenant is in the hierarchy, tenant validation rules permit service provider references.

A service provider user asking to create or update an object is subject to the same restrictions as tenant users, except that service provider users can be authorized to create or update tenanted public objects. The defined role of the service provider user controls this authorization. A service provider user with authorization to multiple tenants who is creating a tenanted object must specify the tenant directly or indirectly.

User Interface Impact

Implementing multi-tenancy changes the user interface, depending on the authorization and tenant access associated with the role for the user.

Note: For more information about creating a user role and assigning a role to a user, see the *Administration Guide*.

Tenant Users

A tenant user who is restricted to a single tenant and who is not an administrator has the following user interface changes:

- Any user belonging to more than one tenant can select a tenant in a drop-down list when entering information and when generating a report.

  Note: If you do not want a user to select a tenant when generating a report, you can remove the tenant drop-down list from the report. For more information about removing the tenant drop-down list, see the *User Guide*.

- Any user having read access to more than one tenant has a Tenant Name column in search results.

How to Implement Multi-Tenancy

Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single implementation of CA APM. Tenants only interact with each other in defined ways, as specified by their roles and tenant hierarchies. Typically, unless granted access by a role or hierarchy, each tenant views the CA APM implementation as solely for its own use and cannot update or view data for another tenant.

To implement multi-tenancy in CA APM, complete the following steps:

1. Verify that the CA CASM service is started (see page 22).
2. Verify that the user implementing multi-tenancy is assigned to a role in which multi-tenancy administration access is enabled.

   Note: For information about defining roles and assigning a role to a user, see the *Administration Guide*.
3. Enable multi-tenancy (see page 93).
4. Define tenants, subtenants, and tenant groups (see page 93).
5. Restart the CA APM web server and application server.
6. Log in to the product using the privileged username (typically *uapmadmin*) and complete the following steps:
   a. Define user roles with tenant access.
   b. Define contacts, or import and synchronize users.

      Note: For information about importing and synchronizing users, see the *Administration Guide*.
   c. Authorize users to use the product.

      Note: For information about authorizing users, see the *Administration Guide*.
   d. Assign contacts to user roles.
7. Log in to the product using the privileged username and verify that the multi-tenancy restrictions are enforced.

Enable Multi-Tenancy

Enable multi-tenancy so multiple independent tenants (and their users) can share a single implementation of CA APM. Before you enable multi-tenancy, define tenants, subtenants, tenant groups, and create user roles and assign users to roles. As soon as you enable multi-tenancy, multi-tenancy enforcement is enabled. Multi-tenancy enforcement means that when an object is tenant-required, you cannot save a record without meeting the tenant restrictions.

Note: For more information about creating users roles and assigning roles to users, see the *Administration Guide*.

To enable multi-tenancy

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. Click Edit.

3. In the Status drop-down list, select one of the following options:

   off

   Disables multi-tenancy.

   on

   Enables multi-tenancy.

4. In the Maximum Tenant Depth field, specify the maximum depth allowed for a tenant hierarchy.

5. Click Save.

   Multi-tenancy is enabled.

6. Restart the web server and application server.

More information:

Tenancy Management Page Cannot Be Displayed Browser Error Appears (see page 147)

Tenant, Subtenant, and Tenant Group Administration

Define the tenants, tenant groups, and subtenants to share a single implementation of CA APM. Multi-tenancy allows tenants to share hardware and application support resources, which reduces the cost of both, while gaining many benefits of an independent implementation.

Define a Tenant

You can define as many tenants as required to manage multiple separate enterprises that provide support to clients. Define a tenant before an instance of a tenant-required object can be updated.

Important! The first created tenant, the service provider, is the primary tenant (owner) in a CA APM multi-tenancy implementation. The service provider tenant cannot have a parent tenant. After you define the service provider tenant, log out of the product and log in again as a member of the service provider. We recommend that you log in as the privileged user (uapmadmin), because this user automatically belongs to the service provider tenant.

To define a tenant

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.

   The Tenants page appears.

3. Click Create Tenant.

   The Create New Tenant page appears.

4. Enter the tenant information. The following fields require explanation:

   Tenant Number

   (Information Only) Displays the tenant number. CA APM does not use this field.

   Record Status

   Sets the tenant to active or inactive. After you define the service provider tenant, this option is read-only for the tenant.

   Terms of Usage

   (Information Only) Displays the terms of usage statement for the tenant. CA APM does not use this field.

   Parent Tenant

   Specifies another tenant above this tenant, making this tenant a *subtenant* in a tenant hierarchy.

   Subtenants Allowed

   Allows this tenant to have subtenants. The tenant cannot modify the setting.

   Tenant Depth

   (Information Only) Indicates the tenant depth of this tenant.

Logo

(Information Only) Displays the URL for an image file that contains the logo for the tenant, which can be any web image type. CA APM does not use this field.

Contact

Displays the Contact lookup page.

Location

Displays the Location lookup page.

5. Click Save.

   The tenant is defined.

Update a Tenant

When necessary, you can update the information for an existing tenant.

To update a tenant

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.

   The Tenants page appears.

3. Search to find the tenant that you want to update.

   All tenants matching the search criteria appear in the Tenant List.

4. Click the tenant that you want to update.

   The tenant information appears.

5. Click Edit.
6. Enter the new information for the tenant.
7. Click Save.

   The tenant is updated.

Make a Tenant Active

When users must see and enter information for a particular tenant that is inactive, you can make the tenant active. For example, the service provider did not receive payment for services provided to a particular tenant. Based on the service agreement, the service provider makes the tenant inactive and stops offering services until payment is made. After the tenant provides payment for the services, the service provider makes the tenant active.

To make a tenant active

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.

   The Tenants page appears.

3. Search to find the tenant that you want to make active.

   All tenants matching the search criteria appear in the Tenant List.

4. Click the tenant that you want to make active.

   The tenant information appears.

5. Click Edit.

6. In the Record Status drop-down list, select Active.

7. Click Save.

   The tenant is active.

How to Initialize a New Tenant

As the service provider, you can define a standard set of data for a new tenant, such as cost centers, cost types, and departments. For information about how to import data for tenants, see the *Administration Guide*.

Define a Tenant Group

You can define a tenant group to classify, manage, and control access to tenants. For example, you can assign asset managers to a tenant group containing tenants belonging to a particular geographic location.

To define a tenant group

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant Group.

   The Tenant Groups page appears.

3. Click Create Tenant Group.

   The New Tenant Group Detail page appears.

4. Enter the tenant group information.

5. Click Save.

   The tenant group is defined.

6. Click Assign Tenants.

   The Tenant Search page appears.

7. Search and select the tenant that you want to add to the group.

   The tenant is added to the group.

Update a Tenant Group

You can update a tenant group to manage the group members and detail information.

To update a tenant group

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant Group.

   The Tenant Groups page appears.

3. Search to find the tenant group that you want to update.

   All tenant groups matching the search criteria appear in the Tenant Group List.

4. Click the tenant group in the list.

   The Tenant Group Detail page appears.

5. Click Edit.

6. Enter the new information for the tenant group.

7. (Optional) Click Assign Tenants to add a tenant to the group.

   Note: Adding or removing a tenant also adds or removes the subtenants of that tenant.

8. Click Save.

   The tenant group is updated.

Tenant Hierarchies

A *tenant hierarchy* is a structured tenant group that is system-created or modified when you assign a parent tenant to a tenant. The tenant becomes a subtenant of the parent and higher tenants (if any) in that hierarchy.

Note: The service provider can create multiple unrelated hierarchies, or none. Even in a system with tenant hierarchies, you can define standalone tenants.

CA APM supports a tenant hierarchy of unlimited depth. However, the service provider can specify a limit on the total number of tenants and the depth of tenant hierarchies (default is four levels). The service provider also determines whether individual tenants can have subtenants.

Note: Although not required, the service provider can participate in tenant hierarchies. The service provider cannot have a parent tenant.

Define a Subtenant

Subtenancy allows you to define and modify tenant hierarchies for organizational and data-sharing purposes. To place a tenant into a tenant hierarchy, you specify a parent tenant for the tenant.

To define a subtenant

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.

   The Tenants page appears.

3. Click Create Tenant.

   The Create New Tenant page appears.

4. Enter the subtenant information. The following fields require explanation:

   Parent Tenant

   Specifies another tenant above this tenant, making this tenant a *subtenant* in a tenant hierarchy.

   Note: The Parent Tenant drop-down only displays tenants that are allowed to have subtenants.

5. Click Save.

   The tenant is a subtenant of the parent tenant.

   Note: When a tenant becomes a subtenant, the tenant belongs to the subtenant group of the parent tenant, in addition to its other subtenants (if any), and so on. The parent tenant joins the supertenant group of its new subtenant, in addition to its other supertenants (if any), and so on. Each joins the related tenants group of the other.

Update a Subtenant

When necessary, you can update the information for an existing subtenant.

To update a subtenant

1. Click Administration, Tenancy Management.

   The Multi-Tenancy Administration page appears.

2. On the left, click Tenant.

   The Tenants page appears.

3. Search to find the tenant that you want to update.

   All tenants matching the search criteria appear in the Tenant List.

4. Click the tenant in the list. The subtenant name appears in the Name column of the Tenant List.

   The tenant information appears.

5. Click Edit.

6. Enter the new information for the subtenant.

7. Click Save.

   The subtenant is updated.

Product-Maintained Tenant Groups

The product generates and maintains the following tenant groups automatically for each tenant in a tenant hierarchy (*tenant* is the tenant name):

- *tenant*_subtenants (tenant, its *child* tenants, and their lower subtenants)
- *tenant*_supertenants (tenant, parent tenant and its higher supertenants)
- *tenant*_relatedtenants (entire single hierarchy)

System-maintained groups can be used like user-defined tenant groups. However, only the name and description can be modified.

Chapter 6: Integrating with Other Products

This section contains the following topics:

CA Business Intelligence Integration

CA Business Intelligence is a set of reporting and analytic software that several CA products use to present information and support business decisions. CA products use CA Business Intelligence to integrate, analyze, and present vital information required for effective enterprise IT management.

CA Business Intelligence installs SAP BusinessObjects Enterprise as a stand-alone product that provides a complete suite of information management, reporting, query, and analysis tools. The installation operates independently of any CA products, allowing the products to share the same CA Business Intelligence services.

CA products leverage an extensive set of business intelligence capabilities, including reporting, query, and analysis, using BusinessObjects Enterprise technology. CA APM provides predefined BusinessObjects Enterprise reports. For more information about the predefined reports, see the *User Guide*. CA Business Intelligence provides users with additional configurable reporting capabilities.

The BusinessObjects Enterprise installation media and documentation are delivered with the CA APM installation media and documentation.

Important! You must install CA Business Intelligence before you install CA APM.

How to Integrate CA APM and CA Business Intelligence

Important! You must install CA Business Intelligence before you install CA APM.

CA APM supplies the required data to get started with BusinessObjects Enterprise reports. After you install BusinessObjects Enterprise and CA APM, you perform required setup tasks before using reports. To integrate CA APM with BusinessObjects Enterprise, complete the following steps:

1. Become familiar with BusinessObjects Enterprise, including the documentation, so that you can administer and use the product. You must be able to perform at least the following functions:
   - Install CA Business Intelligence, which installs BusinessObjects Enterprise.
   - Use predefined reports in BusinessObjects Enterprise.
2. Install CA Business Intelligence BusinessObjects Enterprise and make a note of the following login credentials and connection information, which you will be asked to enter during the CA APM installation:
   - BusinessObjects Enterprise administrator ID
   - BusinessObjects Enterprise administrator password
   - BusinessObjects Enterprise Central Management Server (CMS) port. The CMS maintains a database of information about your BusinessObjects that you use with CA Business Intelligence. The default CMS port is 6400.
3. If you are using Oracle as the CA MDB, define an Oracle Net Service Name (NSN) on the server where CA Business Intelligence is installed. Make a note of the NSN, which you will be asked to enter during the CA APM installation.
4. Verify that BusinessObjects Enterprise is installed by starting BusinessObjects Enterprise.
5. Install CA APM (see page 11). The CA APM installation installs and configures the BIAR file for both the Oracle and the SQL Server databases. The BIAR file includes the CA Business Intelligence universe, predefined reports, and the CA APM default administrative user (uapmadmin).

   Note: When you install CA APM, you enter the BusinessObjects Enterprise login credentials, BusinessObjects Enterprise CMS port, and the Oracle NSN that you recorded. If .NET Framework is not installed on the CA Business Intelligence server, enter 6400 when prompted for the CMS port.
6. Become familiar with and use the predefined reports. For more information about the predefined CA APM reports, see the *User Guide*.
7. Follow these best practices when maintaining and using BusinessObjects Enterprise:
   - Install and maintain one universe for each CA product.
   - Do not modify the default universe. Instead, copy the universe and modify the copy. Otherwise, any custom changes you make may not be retained when you apply service packs, patches, and other updates.

- Back up your changes before you apply service packs, patches, and other updates to your custom universe.
- If reports do not work correctly, verify that the CMS is operating.
- Do not overwrite predefined reports.
- Always use a predefined report as a base to build a custom report, which helps maintain consistent formatting in all reports.
- Remember that administrators can modify all the reports and create new reports based on the existing universe. However, administrators cannot add any reports to the existing CA APM folder.
- Administrators and end users should not change predefined reports because any changes to those reports are applied to all other users using the same CA Business Intelligence instance. Instead, create custom folders, copy the reports to the custom folders, rename and customize the reports.
- Both administrators and users must add new reports that they create to their custom folders.

Report Configurations and Product Updates

When you install updates (patches, service packs, or other updates) to CA APM, the update process overwrites the existing product components, including in some cases the reporting components. As a result, any reporting configurations you previously made may be lost. However, CA Technologies provides you with a method to retain your report configurations when you apply CA APM updates. Follow the instructions in a CA Technologies-provided white paper, which you can open from http://ca.com/support.

Under Technical Support, navigate to the product page for CA Technologies IT Asset Manager. Search the Recommended Reading list for *White Paper: Reporting Components Upgrade and Version Control to Retain Customizations*. You can safeguard your report configurations by implementing the strategy outlined in the white paper.

Note: See the *CA Business Intelligence Implementation Guide* for information about configuring reports.

CA EEM Integration

CA APM uses CA EEM for authentication. You must install CA EEM before you begin the product installation.

Other products that need CA EEM for authentication can use the same CA EEM server that CA APM uses.

- You can use CA EEM to manage security centrally for multiple CA Technologies products. Specify the name, location, and login credentials for the existing server during the CA APM installation process.
- You can also manage CA APM security independently from other CA Technologies products. Install CA EEM on any single application or web server other than the one where the existing CA EEM is installed.

CA CMDB Integration

This section explains how to integrate CA APM with CA CMDB Release 12.7 and CA CMDB that is included in CA Service Desk Manager Release 12.7.

CA CMDB is a comprehensive, integrated solution for managing the IT components and services in an enterprise and their relationships, in heterogeneous computing environments. CA CMDB makes it possible to provide and store reliable, up-to-date information about assets, known as configuration items (CI), and their relationships with each other. These relationships form the basis for impact analysis, an important tool for controlling change within an organization.

CA CMDB integrates with CA APM in several areas, including the following areas:

- The CA APM audit history records can include all of the changes that have been made to asset/CI records by CA Service Desk Manager, CA CMDB, and CA APM.
- When CA Service Desk Manager and CA CMDB are installed, the asset/CI audit history records include any CA APM audit history records on the CA CMDB Versioning tab.
- When you define an asset in CA APM, you can categorize and control the asset and CI records by selecting or clearing the Asset and CI check boxes. This flexibility is provided because CIs that CA CMDB creates may not be relevant to CA APM. Conversely, assets that CA APM creates may not be relevant to CA CMDB.

- CA APM can extend the fields on an asset/CI within the context of *asset families*. The extended fields can be shared in CA APM. For example, a CA APM administrator can configure the Asset page and define an asset extended field to let users view and update a CI that is created in CA Service Desk Manager and CA CMDB.
- You can define an event on a field that is shared with CA CMDB in CA APM and trigger the event in either CA APM or CA CMDB. For more information about managing events and notifications, see the *User Guide*.
- A CA Service Desk Manager and CA CMDB user can define a Management Data Repository (MDR) and allow the CA CMDB CI to launch the corresponding asset in CA APM.

How to Integrate CA APM and CA CMDB

When you integrate CA APM and CA CMDB, you integrate and delineate the assets that CA APM manages from the configuration items (CIs) that CA CMDB manages in a simple and concise manner. CA APM users can move to a shared classification model for the assets and CIs. To integrate CA APM and CA CMDB, complete the following steps:

1. Share asset and configuration item audit history records (see page 105).
2. Categorize the asset and configuration item records (see page 106).
3. Define an asset extended field (see page 108).
4. Define an event on a shared field (see page 110).
5. Define a Management Data Repository (MDR) from CA Service Desk Manager and CA CMDB (see page 110).

Share Asset and Configuration Item Audit History Records

To integrate CA APM and CA CMDB, the CA APM audit history records can include all of the changes that were made to asset/CI records by CA Service Desk Manager, CA CMDB, and CA APM. In addition, when CA Service Desk Manager, CA CMDB, or both are installed, the asset/CI audit history records in CA CMDB (Versioning tab) includes any CA APM audit history records.

CA CMDB 11.2 and greater includes audit history records from CA APM. The audit history records are updated in both CA CMDB and CA APM when the CA Asset Portfolio Management - Event Service service is started. For more information, see Start the Services (see page 22).

Categorize the Asset and Configuration Item Records

In this step to integrate CA APM and CA CMDB, you can categorize and control the asset and CI records when defining an asset in CA APM by selecting or clearing the Asset and CI check boxes. This flexibility is provided because CIs that CA CMDB creates may not be relevant to CA APM and conversely, assets that CA APM creates may not be relevant to CA CMDB.

Consider the following information when using these check boxes:

Default Values

- All new asset records that CA APM creates are initially set both as an Asset only and Managed by CA APM. On the New Asset page in CA APM, the Asset check box is selected, the Managed by CA APM check box is selected, and the CI check box is not selected.
- All asset records that CA CMDB creates (with or without CA Service Desk Manager) are initially set to CI only. On the CI pages in CA CMDB, the CI? column heading is set to Yes and the Asset? column heading is set to No.
- Both CA APM and CA CMDB have the Asset and CI fields available on the New Asset and CI pages. However, the Managed by CA APM check box is only viewable in CA APM. The existing audit and security features for each product applies to these check boxes.

Appearance

- The Asset and CI fields appear in CA APM and CA CMDB even when other CA Technologies products are installed. The Asset and CI fields do not appear in CA Service Desk Manager when CA CMDB is not installed.
- The CA APM administrator can configure the user interface and move the Asset and CI fields to a new location, make the fields read-only, required, or optional, and hide the fields.

  Note: For more information about configuring the user interface, see the *Administration Guide*.

Viewing and Updating

CA CMDB

- By default, the CA CMDB analyst and administrator can update the Asset and CI field values.
- CA CMDB, by default, does not allow the Asset? value to be changed when the Asset? value is set to Yes.

CA APM

- By default, CA APM sees asset and CI records.
- The CA APM administrator can configure the user interface and move the Asset and CI check boxes to a new location, make the check boxes read-only, required, or optional, and hide the check boxes. After you select the CI check box and save the asset, the CI check box is not available and you cannot change the setting.

  Important! We strongly recommend that you configure the CI check box in CA APM as read-only and restrict changes to the check box to only the CA CMDB analyst and administrator.
- An asset in CA APM in which the Managed by CA APM check box is selected is always an asset. You cannot save an asset in CA APM in which the Managed by CA APM check box is selected without also selecting the Asset check box.

Searching

CA CMDB

- The CA CMDB search initially displays, by default, all records. However, an option is provided to filter records.

  Note: If CA Service Desk Manager is installed, the same default search rules apply.

CA APM

- The default asset search includes a drop-down list for Managed by CA APM, CI, and Asset. This flexibility is provided so that you can differentiate between assets and CIs.

Hardware Reconciliation

Hardware reconciliation analyzes all asset and CI records. Searches provide a way to view any CIs that are related to discovered assets as the result of running hardware reconciliation. A CA APM user can view the exceptions and determine whether they want to select the Asset check box. As a result of selecting the Asset check box, the asset records are available in a CA APM asset search.

Define an Asset Extended Field

In this step to integrate CA APM and CA CMDB, CA APM can extend the fields on an asset within the context of *asset families*. The extended fields can be shared in CA APM. For example, a CA APM administrator can configure the Asset page and define an asset extended field to let users view and update a CI that is created in CA Service Desk Manager and CA CMDB.

Important! These steps work only the first-time you complete the wizard and define the asset extended field. Before you define the extended field, verify that you have the following information from the usp_owned_resource table in CA CMDB for reference: table name, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, and field size. After you complete the wizard, you can configure the extended field like any field in CA APM.

Example: Define an Asset Extended Field for Warranty Start Date

In this example, you define an asset extended field for Warranty Start Date. In CA Service Desk Manager/CA CMDB on the Inventory tab, you view the label in the CI as Warranty Start Date. Next, you view the information for the associated nr_wrty_st_dt column from the usp_owned_resource table in CA CMDB. In this example, the nr_wrty_st_dt column format is integer, the field name is nr_wrty_st_dt, the attribute name is nr_wrty_st_dt, and the field size is 4. Record and enter this information exactly as it appears in the appropriate Format, Field Name, Attribute Name, and Field Size fields in the wizard. We also recommend that to avoid confusion, you use the same label for the CI (Warranty Start Date) on the Label field in the wizard.

To define an asset extended field

1. Determine the CA Service Desk Manager and CA CMDB extension table name and database field name by reviewing the CA Service Desk Manager and CA CMDB schema files.

   Note: For more information about the CA Service Desk Manager and CA CMDB schema files, see the CA Service Desk Manager and CA CMDB documentation.

2. Log in to CA APM using login credentials in which you have permissions to define an extension.
3. Click Asset, New Asset.
4. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

5. In the Configuration Information area of the page, define and save a global configuration.
6. Click Add Extension.

   A wizard appears.

7. Follow the on-screen instructions to enter the information for the extended field.
8. In the Type page of the wizard, complete the following steps:
   a. Select the Simple Field option.
   b. Select the part of the page on which the new field appears.
   c. Select the Across all extended types check box.
   d. Click Next.
9. In the Fields page of the wizard, complete the following steps:

   Important! Enter the column information from the usp_owned_resource table in CA CMDB. We also recommend that to avoid confusion, you use the same label for the CI on the Label field.

   a. Click Add Field.
   b. Enter the field label to appear on the page.
   c. Select the data format.
   d. Enter the database field name.
   e. Enter the attribute name.
   f. Enter the field size.
   g. (Optional) Enter a description for the field.
   h. Specify whether an entry for the field is required.
   i. Click the checkmark icon to save the field.

      The product displays the field information you enter.
   j. Click Next.
10. In the Summary page of the wizard, review the field information and click Save and Exit.
11. Verify that the field appears on the Asset page.
12. Click Save Configuration.

    All users see the extended field on the page. You can define an event in CA APM and trigger the event in either CA APM or CA CMDB. For more information about managing events, see the *User Guide*.

Define an Event on a Shared Field

You can define an event in CA APM on any field that is shared between CA APM and CA CMDB. When the criteria for the event occurs by a change in CA Service Desk Manager/CA CMDB or CA APM, the event will complete and the notification will be sent. For example, you can define an event on the Asset page for the Contact field. If the event is a change event, the event can be completed when you change the Contact field in either the asset or the related configuration item (CI). Once the event has completed, a notification will be sent.

Note: For more information about managing events and notifications, see the *User Guide*.

Define a Management Data Repository (MDR) from CA Service Desk Manager and CA CMDB

In this step to integrate CA APM and CA CMDB, a CA Service Desk Manager and CA CMDB user can define a Management Data Repository (MDR) and allow the CA CMDB CI to launch in context the corresponding asset in CA APM.

To define a MDR from CA Service Desk Manager and CA CMDB

1. In the CA Service Desk Manager web interface, log in as an administrator.
2. Select the Administration tab. From the Administration browser, select CA CMDB, MDR Management, MDR List.
3. Click Create New.

   The MDR Provider definition appears.
4. Enter the following required MDR provider information:

   Button Name

   Specify *ITAM* as the button name.

   MDR Name

   Specify *ITAM* as the MDR name.

   MDR Class

   Specify *GLOBAL* as the MDR class.

   Hostname

   Specify the CA APM server name by using the network address or the DNS name of the CA APM web server.

   Important! The MDR provider form automatically populates the URL for Launch in Context field based on the information that you provide, so you do *not* enter a value for this field.

5. Click Save.

   The CA APM MDR provider is defined.

6. In CA CMDB, define a CI.
7. Click the Attributes tab in the CI detail form.
8. Click the ITAM button that you previously defined.

   The corresponding asset in CA APM appears.

CA Process Automation Integration for a Notification Process

CA APM and CA Process Automation integrate to let you set up and configure a notification process that delivers notifications to specific recipients after a defined event occurs. CA APM provides email notification processes with the product. These processes are delivered in files that are included on the product installation media. You import the files into CA Process Automation and specify process parameters in CA Process Automation and CA APM.

How to Set Up the CA Process Automation Notification Process

Use the following steps to set up the email notification processes that are provided with CA APM.

1. Install CA APM and CA Process Automation.
2. In CA Process Automation, import the workflow provider notification process files (see page 112).
3. In CA Process Automation, configure the mail server (see page 112).
4. In CA Process Automation, modify the settings for the workflow process parameters (see page 113).
   a. Change the default email address for the administrator (Admin_Email_To parameter) to specify your required setting.
   b. Change the default CA APM URL (ITAM_URL parameter) to specify your required setting.
   c. Change the default CA Process Automation URL (ITPAM_URL parameter) to specify your required setting.
   d. (Optional) Change any of the other parameters for which you want to specify your required settings.

5. In CA APM and CA EEM, permit CA APM users to use CA Process Automation (see page 115).
6. In CA EEM, create CA Process Automation user accounts for any non-CA APM users.
7. In CA APM, specify the workflow process parameters when you define an event.

   Note: For information about defining an event in CA APM, see the *User Guide*. For information about using CA Process Automation and CA EEM, see the CA Process Automation and CA EEM documentation.

Import the Workflow Provider Notification Process Files

CA APM provides default email notification process files. You import these files into CA Process Automation before you can set up and can configure email notifications in the products.

Note: For more information about importing and working with the files, see the CA Process Automation documentation.

Follow these steps:

1. Log in to CA Process Automation as the administrator.
2. Navigate to the CA Process Automation client.
3. Locate the ITAM.xml file on the CA APM installation media using the following path:

   `CD1\SetupFiles\ITPAM\`
4. Import the ITAM.xml file into the **/** node.

   Note: In CA Process Automation Release 3.1, you import the XML file from the client. In Release 4.0 SP1, you import the XML file from the Library tab.

   Select the import options to set the imported versions as current and to make the imported custom operators and sensors available.

   The notification process files are imported into the default /ITAM folder.

Configure the CA Process Automation Mail Server

To implement email notifications between CA Process Automation and CA APM, configure the mail server for CA Process Automation.

Note: For specific instructions on configuring the CA Process Automation alert module to set up the mail server, see the *CA IT Process Automation Manager Administration Guide*.

1. Log in to CA Process Automation as the administrator.
2. Navigate to the CA Process Automation client.

3. Navigate to the library browser.
4. Locate and lock the default environment.
5. Locate the alert module and clear the inherit check box.
6. Specify the SMTP (mail) server.

   Example: mail.company.com
7. Specify the From address.

   Example: admin@company2.com
8. Save the changes.
9. Unlock the default environment.

   The changes require a few minutes to take effect.

Note: You can send an email notification to an external email address if your SMTP (mail) server settings permit email delivery to the external address. Check your mail server settings to verify if you can send email to external addresses.

Modify CA Process Automation Workflow Process Parameters

After you install CA APM and CA Process Automation and import the notification process files into CA Process Automation, the default workflow process parameters are defined in CA Process Automation. You can modify the default process parameters to include your required settings. You provide actual (hard-coded) values for the process parameters. You must verify that the values you enter are valid.

You can modify the notification process parameters in the data set that applies to all notification processes or in the individual process start request forms. The parameters you specify for an individual process override the parameters in the main data set for that process.

Note: You specify some of the notification process parameters for the workflow provider when you define an event in CA APM. For more information about specifying process parameters in CA APM, see the *User Guide*.

To modify CA Process Automation workflow process parameters

Important! CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

1. Log in to CA Process Automation and navigate to the CA Process Automation client.
2. In the ITAM folder, locate the data set that is named Dataset.

3. Enter the information for the parameters.

   The following fields require explanation:

   Ack_Interaction_Form_Full_Path

   Full path to the file that contains the acknowledgment interaction form in CA Process Automation. The email notification recipient uses this form to acknowledge receipt of the notification. Each workflow process must have a unique user interaction form and a unique path to the form. You can find the acknowledgment interaction form files that are provided with the product in the folder that contains the processes and main data set (/ITAM or the folder where you imported the processes).

   Admin_Email_CC

   Email address of the copy recipients for the email that is sent to the administrator when a notification error occurs.

   Admin_Email_To

   Email address of the administrator for the email that is sent when a notification error occurs. Change the default value to your required setting.

   Log_Folder_Path

   Full path of the error log file that is created when an error occurs with the notification process. If you do not specify a path, the log file uses the default CA Process Automation log file path.

   ITAM_Username

   User name to log in to CA APM. CA Process Automation requires access to CA APM for information about notification recipients and escalation.

   ITAM_Password

   User password to log in to CA APM. CA Process Automation requires access to CA APM for information about notification recipients and escalation.

   Admin_Email_Subject

   Subject for the email that is sent to the administrator when a notification error occurs. This parameter can be set in the main data set or in the individual process start request form.

   Admin_Email_Header

   Header or introduction for the email that is sent to the administrator when a notification error occurs (for example, "Hello"). This parameter can be set in the main data set or in the individual process start request form.

   Admin_Email_Footer

   Signature for the email that is sent to the administrator when a notification error occurs (for example, "Thank You"). This parameter can be set in the main data set or in the individual process start request form.

Log_File_Name

Name of the error log file that is created when an error occurs with the notification process. The email that is sent to the administrator when a notification error occurs contains the log file name. If you do not specify a name, the log file uses the following default CA Process Automation log file name:

*process name_process instance number.*log

ITAM_URL

CA APM URL that CA Process Automation uses to access CA APM for information about notification recipients and escalation. Change the default value to your required setting.

Example:

`http://ITAMAPPSERVER:99/ITAMService/Service.asmx`

ITPAM_URL

CA Process Automation URL that is included in the email notification message. Change the default value to your required setting.

Example:

`http://PAMSERVER:8080/itpam`

4. Save the changes in CA Process Automation.

Note: For information about setting up a notification process, see your workflow provider documentation.

Permit CA APM Users to Use CA Process Automation

The CA APM users who receive notifications need to access CA Process Automation to acknowledge the notifications. These users need to have permission to use CA Process Automation. You permit users to use CA Process Automation by performing steps in CA APM first and then in CA EEM. In CA APM you define and authorize users to log in to and use CA APM. In CA EEM, you permit the authorized CA APM users to use CA Process Automation.

To permit CA APM users to use CA Process Automation

1. Log in to CA APM.
2. Verify that both new users and existing users are authorized to log in to and use CA APM.

   Note: For information about defining and authorizing new users and authorizing existing users in CA APM, see the *Administration Guide*.

   The product defines and authorizes the CA APM users. CA EEM now includes the CA APM users in the list of available users.

3. Log in to CA EEM, selecting CA Process Automation from the application drop-down list.

   Important! You must select the CA Process Automation application when you log in to CA EEM to permit CA APM users to use CA Process Automation.

4. Select a CA APM user from the list of all users and click the application user details for the user.

5. Select a CA Process Automation user group for the user and save the selection.

   Note: For information about using CA EEM to add applications to user details, see the CA EEM documentation.

   The CA APM user can now access and use CA Process Automation.

Required Indicators and Multiple Line Text Fields for Parameters

The default notification processes that are delivered with the product contain the parameters that appear on the product Event Definition user interface and the parameters that you specify in the workflow provider. The default processes also contain XML formatting that lets you display a required indicator and a multiple line text field on the product user interface. These items are not readily available from the workflow provider, and so they are specified in the process. In the CA Process Automation start request form for each default process, the following XML statement appears before the Description of each user interface parameter:

```
<FieldDescriptor><IsRequired>true_or_false</IsRequired><Length>number</Length></FieldDescriptor>
```

IsRequired

Specifies if the parameter is required (true) or not required (false). If the parameter is required, the product displays the standard required indicator on the user interface.

Example: <FieldDescriptor><IsRequired>true</IsRequired></FieldDescriptor>

Length

Specifies the length of the parameter text entry field. To define a multiple line text field, specify a value greater than 255.

Example: <FieldDescriptor><Length>275</Length></FieldDescriptor>

You can change the default notification processes that are delivered with the product, and you can also create your own new notification process. To include information about the required indicator and field length in your changed or new process, you must insert the XML statement before the Description of each user interface parameter in your process.

Note: If you are creating a new notification process, you must have a corresponding start request form for the process. For information about changing or creating notification processes, see your workflow provider documentation.

CA Process Automation Integration for a Data Importer Process

CA APM and CA Process Automation integrate to let you set up and configure a Data Importer process. This integration uses a sample data import XML file that you import into CA Process Automation and integrate with an overall process workflow. The Data Importer process launches the Data Importer and executes a data import.

Note: This integration uses CA Process Automation and a sample data import XML file that is company-provided. You can also use any other workflow provider to create your own overall workflow and Data Importer process.

How to Set Up the CA Process Automation Data Importer Process

Use the following steps to set up the Data Importer process:

1. Install CA APM and CA Process Automation.
2. Log in to the application server where you installed CA APM.
3. Access the following folder on the CA APM application server where the Storage Manager Service is installed.

   `[ITAM Root Path]\Storage\Common Store\Import`
4. Locate the Import_Automation_Workflow.xml file.
5. In CA Process Automation, import the Import_Automation_Workflow.xml file.
6. In CA Process Automation, integrate the Import_Automation_Workflow.xml into your overall process workflow.
7. In CA Process Automation, modify the settings for the Data Importer process parameters.
   a. Change the default Import Service URL to match your required setting.
   b. Change the default CA APM user ID and password to your own settings.

c. Change the default data import name to match your data import.

d. Specify the data file name that corresponds to your data import.

Note: For information about using CA Process Automation, see the CA Process Automation documentation.

Modify CA Process Automation Workflow Process Parameters

After you install CA APM and CA Process Automation and import the Import_Automation_Workflow.xml file into CA Process Automation, the default workflow process parameters are defined in CA Process Automation. You can modify the default process parameters to include your required settings. You provide actual (hard-coded) values for the process parameters. You must verify that the values you enter are valid.

You can modify the process parameters in the main data set or in the individual process start request forms. The parameters that you specify for an individual process override the parameters in the main data set for that process.

Follow these steps:

Important! CA APM and CA Process Automation do not validate the information that you enter for the parameters. You must verify that your input is valid and that you entered the data in the correct format.

1. Log in to CA Process Automation and navigate to the CA Process Automation client.
2. Enter the information for the Data Importer parameters. The following fields require explanation:

   ITAMImportServiceURL

   Specifies the complete URL path where the Import Service is running.

   Example:

   `http://server/ImportService/ImportService.svc`

   username

   Specifies the CA APM user ID.

   password

   Specifies the CA APM user password.

Importname

Specifies the name of the data import that you want to execute.

FilePath

Specifies the complete path and name of the data file that is associated with your data import.

Example:

```
C:\\CAITAMCostcenter.csv
```

3. Save the changes in CA Process Automation.

Note: For information about setting up a process in CA Process Automation, see your CA Process Automation documentation.

CA Service Catalog Integration

CA Service Catalog integrates with CA APM to let you associate requested items from a service request with CA APM assets. You can associate CA APM assets with items requested from CA Service Catalog during request fulfillment. Assets that are already assigned to a request can be viewed and can be removed from the request, if needed. In addition, you can deny the fulfillment of a request for assets.

Important! CA APM and CA Service Catalog must share the same CA MDB and the same CA EEM for the integration to work properly.

Note: For information about fulfilling requests from inventory, see the *User Guide*. For information about creating and managing requests in CA Service Catalog, see the *CA Service Catalog Integration Guide*.

Chapter 7: Implementing CA SAM with CA APM

This section contains the following topics:

Overview

CA APM coordinates with CA SAM to allow you to perform software asset management functions. CA SAM is the next evolution of software asset and compliance management, superseding CA Software Compliance Manager (CA SCM). See the product support site on CA Support Online for more information about the plans for CA Software Compliance Manager.

Important! We do not recommend that you manage software assets in CA APM. To take advantage of the enhancements that CA APM Release 12.9 provides, we recommend that you use CA SAM to manage your software assets and licenses.

CA SAM provides the following advantages:

- Supports the process of determining your software license compliance position by comparing the number of available licenses with the number of used licenses.
- Integrates a software license import function into the CA SAM user interface.
- Facilitates the creation and maintenance of a software license catalog with detailed commercial information about the licenses.
- Assigns installation and usage data to defined products in the software license catalog.
- Performs software product recognition.
- Permits financial analysis of product prices, license costs, and contract payments (this function is available through an additional module).

If you implement both CA APM and CA SAM, you can coordinate the management of both hardware and software assets in your organization. CA APM maintains hardware asset data and CA SAM maintains software asset and license data. Common data that both CA APM and CA SAM require is shared.

CA APM and CA SAM Data Synchronization

When you implement CA APM with CA SAM, CA APM and CA SAM share data that is required for hardware and software asset management. To maintain the integrity of the data and of the asset management process, data must be synchronized between CA APM and CA SAM. Data synchronization ensures that objects that are the same in both CA APM and CA SAM contain the same data values. This data synchronization occurs in the following ways:

- Automatic–When you create, update, or delete the following objects in CA APM (through the user interface, web services, or Data Importer), the objects are automatically synchronized in CA SAM. Create, update, or delete the following objects in CA APM only.
  - Company
  - Location
  - Cost center
  - Division
  - Contact

  Important! The CA SAM Administrator must designate these objects as read-only in CA SAM to prevent any unauthorized change and to ensure that data is synchronized correctly. For more information about this requirement, see Data Management Recommendations. For more information about designating objects as read-only in CA SAM, see the CA SAM documentation.

  Note: These objects use the same labels in CA APM and CA SAM, except Contact. In CA SAM, the Contact object is labeled "User".

  For Contact, Company, and Location, the automatic synchronization occurs for specific data types only as shown in the following table:

Object	Automatically Synchronize when Type Is
Contact	User
Company	Internal
Location	NULL

- Manual–When you create or update the following objects in CA APM or CA SAM, synchronize the objects manually. Create or update the following objects in CA APM or CA SAM.
  - Country
  - Region

  For example, if you create a Country object in CA SAM, manually create the same object in CA APM. If you update a Region object in CA APM, manually update that object in CA SAM.

  Note: For more information about manual data synchronization, see the Data Management Recommendations.
- Data Loading–When you upgrade to CA APM Release 12.9 from a previous CA APM Release 12.6 installation, you can load your existing CA APM data for Company, Location, Cost center, Division, and Contact into CA SAM. For more information about data loading, see Load CA APM Data into CA SAM (see page 139).

Note: If you are implementing CA APM with an existing instance of CA SAM, there is existing CA SAM data that has not yet been synchronized. Before you start the automatic synchronization process, synchronize the existing CA SAM data with the CA APM data. For more information, see the following article on the CA SAM product page on CA Support, Recommended Reading section: "How to Synchronize CA APM Data with an existing CA SAM Instance".

How to Configure Data Synchronization

You can configure the automatic data synchronization of CA APM and CA SAM data to suit your particular business needs. You can configure the type and attributes of the objects that are synchronized. You can also configure the criteria that are used to select the data rows for synchronization. To configure the data synchronization, edit the configuration file SAMDataSynchConfig.xml.

Important! The product installation saves the data synchronization configuration file SAMDataSynchConfig.xml with default settings for the data attributes and criteria. You modify this file *only* if you want to customize the default settings.

You can find the data synchronization configuration file in the following Event Service and Application Server folders:

```
<InstallFolder>\CA\ITAM\EventService\SAMDataSynchConfig.xml
```

```
<InstallFolder>\CA\ITAM\Application Server\SAMDataSynchConfig.xml
```

Note: If you change the configuration file in one of the folders, make the same changes to the configuration file in the other folder.

Example: SAMDataSynchConfig.xml Configuration File Structure

The following example shows a section of the configuration file with the following changes to the default attributes and criteria:

- APMCriteria statements (highlighted)–Analyst was added as a criterion for the CA APM contact attribute (contacttype.value). User is the default criterion.
- SamField statements (highlighted)–CA APM contact (contactid) was mapped to the CA SAM user (import_user_id). The default statement (commented out in the example) mapped the CA APM asset owner (resourceownerid) to the CA SAM user (import_user_id).

```
<SamTable apmsyncclass="contact" samsynctable="users" >
    <SamField apmattribute="individualid" samattribute="import_id" />
    <SamField apmattribute="emailid" samattribute="login" />
    <SamField apmattribute="costcenterkey" samattribute="import_level_2_id" />
    <SamField apmattribute="lastname" samattribute="last_name" />
    <SamField apmattribute="firstname" samattribute="first_name" />
    <SamField apmattribute="emailid" samattribute="email" />
    <APMCriteria>
        <Criteria apmattribute="contacttype.value" value="User" />
        <Criteria apmattribute="contacttype.value" value="Analyst" />
    </APMCriteria>

</SamTable>

<SamTable apmsyncclass="asset" samsynctable="devices" >
    <SamField apmattribute="costcenterkey" samattribute="import_org_level_2_id" />
    <SamField apmattribute="locationid" samattribute="import_location_id" />
    <!--<SamField apmattribute="resourceownerid" samattribute="import_user_id"
    />-->
    <SamField apmattribute="contactid" samattribute="import_user_id" />

</SamTable>
```

The following terms in the example require explanation:

SamTable

Specifies the XML node that represents the mapping of the CA APM and CA SAM data objects or table.

Apmsyncclass

Specifies the name of the data synchronization object in CA APM.

Samsynctable

Specifies the name of the database table that the CA APM objects map to in CA SAM.

SamField

Specifies the XML node that represents the mapping of CA APM and CA SAM attributes.

Apmattribute

Specifies the CA APM attribute of the data synchronization object. To generate the name of the attribute, log in to the CA APM database using a database client tool and execute the following query:

```
select attribute_name, class_name, table_name, field_name from arg_attribute_def
where class_name='object_name';
```

Use the value of the attribute_name column as the value for the Apmattribute XML attribute in the configuration XML.

Samattribute

Specifies the field name in the database table that the CA APM attributes map to in CA SAM. For the list of CA SAM objects and attributes, see the *CA Software Asset Manager Administration Manual.*

APMCriteria

Specifies the XML node that holds one or more child criteria nodes.

Criteria

Specifies the XML node that represents the criteria that is applied with the OR connector in the CA APM database table.

Data Synchronization Configuration Limitations

The following limitations apply to the changes that you can make to the data synchronization configuration file:

- You can change the mapping of attributes within a data object. You cannot change the mapping at the object level. For example, you cannot map the CA APM Location with the CA SAM User. You can map the CA APM Location with the CA SAM Location only.

- You can add columns under criteria. For example, the Contact object has User as the default Contact Type. As a result, all the data rows in the Contact object with Contact Type of User are selected for data synchronization. You can add other criteria. The following statements show a sample of how to add criteria:

  ```
  <APMCriteria>
      <Criteria apmattribute="contacttype.value" value="User" />
      <Criteria apmattribute="contacttype.value" value="Analyst" />
      <Criteria apmattribute="costcenter.value" value="NewCostCenter" />

  </APMCriteria>
  ```

  These statements specify the following selection criteria for data synchronization:

  - All Contacts with a Contact Type equal to User or Analyst
  - All Contacts with a Cost Center equal to New Cost Center

- Each criteria XML node can have only one value. For example, the default criteria value for Contact Type is User. More values (for example, “Analyst” or “Employee”) can be added (or removed). However, you cannot have “Analyst, Employee” as the criteria value. Create a criteria XML node for each unique value.

Add an Attribute

You can add an attribute to the data synchronization configuration file. You can also change an existing attribute in the file by editing an existing statement.

Follow these steps:

1. Create a SamField node by adding the following statement under the existing SamField nodes:

   ```
   <SamField apmattribute="attribute_name" samattribute="attribute_name" />
   ```

   Note: Perform the following steps to identify the values that are needed for this statement.

2. Execute the following query on the CA APM database using a database client tool:

   ```
   select class_name, attribute_name, table_name, field_name
   from arg_attribute_def where class_name='object_name';
   ```

3. In the query results, copy the attribute_name value that was generated in the previous step. Paste this value in your new SamField node statement as the apmattribute value.

4. Access the *CA Software Asset Manager Administration Manual,* Data Imports chapter, and locate the field tables in the Formats section.

5. Copy the appropriate field name and paste it in your new SamField node statement as the samattribute value.

   Note: For help with selecting the appropriate CA SAM fields, contact CA Services.

Add Criteria

You can add criteria to the data synchronization configuration file to expand the data values that are selected for data synchronization.

Follow these steps:

1. Create a criteria node by adding the following statement under the existing criteria nodes:

   ```
   <Criteria apmattribute="value" value="value" />
   ```

   Note: Perform the following steps to identify the values that are needed for this statement.

2. Execute the following query on the CA APM database using a database client tool:

   ```
   select class_name, attribute_name, table_name, field_name
   from arg_attribute_def where class_name='object_name';
   ```

3. In the query results, copy the attribute_name value that was generated in the previous step. Paste this value in the new criteria node statement as the apmattribute value.

4. Provide the criteria values by completing the following steps:

   a. Execute the following query:

      ```
      Select field_name, table_name from arg_attribute_def where class_name =
      '<apmsyncclass value>' and attribute_name = <apmattribute value>.
      ```

   b. In the query results, select the field_name from the table_name.

   c. Copy the field value and paste it in the *value="value"* parameter from Step 1.

   Note: Create a separate criteria node for each unique value that you want to synchronize.

How to Implement CA SAM with CA APM

Perform the following steps to implement CA SAM with CA APM:

1. Review the prerequisites (see page 128).
2. Verify the Internet Information Services Installation (see page 129).
3. Install the CA SAM Import and Export Service (see page 27).
4. Configure the CA SAM Import and Export Service (see page 130).
5. Configure the CA APM Event Service for CA SAM (see page 132).
6. Configure the SAM Import Driver (see page 134).
7. Schedule the Windows task for the Hardware Import (see page 135).
8. Start the CA APM Event Service (see page 135).

9. Enable the software asset management capabilities (see page 136).
10. Load CA APM data into CA SAM (see page 139).

Note: To implement CA SAM, you also need to download the latest version of the CA SAM Catalog from CA Support Online and apply the Catalog in CA SAM. You can perform the Catalog download before or after you implement CA SAM with CA APM. For information about the CA SAM Catalog, see the CA SAM documentation.

Review the Prerequisites

Review the following prerequisites to ensure that you can successfully implement CA SAM with CA APM.

- You installed CA APM.

  Important! Verify that the CA APM workflow provider URL is accessible and the corresponding login credentials are valid.

  Note: If your CA APM environment integrates with CA Service Desk Manager (CA SDM), verify that you have enabled the CA SDM audit history.

- You installed CA SAM from the CA SAM installation media. For information about installing CA SAM, see the CA SAM documentation.

  Important! Microsoft .NET Framework 4.0 must be installed also on the CA SAM server.

  Note: If you are using CA SAM to manage software assets for more than 250,000 hardware assets, we recommend the following installation configuration for improved system performance:

  - Install a CA SAM staging server for processing discovery data only. Implement the staging server on a MySQL database for improved performance and scalability.
  - Install the CA SAM production server on either a SQL Server or an Oracle database.
  - Transfer the discovery data to the CA SAM production server when processing is complete on the staging server.

Verify the Internet Information Services Installation

The CA SAM Import and Export Service is installed when you install the new CA APM components that are required for the CA SAM implementation. The CA SAM Import and Export Service installation requires Internet Information Services (IIS) 7.5 with ASP.NET and WCF Activation features enabled. Before you begin the CA SAM Import and Export Service installation, verify that IIS is installed and the required features are enabled on the server where CA SAM is installed.

To verify the Internet Information Services installation:

1. For each application and web server, log in to the server.
2. Open the Control Panel (Administrative Tools, Services).
3. Verify that the IIS Admin service is on the server.

To install IIS version 7.5 on Windows Server 2008 R2:

1. From Server Manager, select Roles.
2. In the Roles Summary area, click Add Roles and click Next.

   The Select Server Roles dialog appears.
3. Select Application Server from the Roles list and click Next twice.

   The Select Role Services dialog for the Application Server role appears.
4. Select Web Server (IIS) Support and, under Windows Process Activation Service Support, select HTTP Activation.
5. If you are prompted to install more role services and features, click Add Required Role Services and click Next twice.
6. Verify that the summary of selections is correct and click Install.
7. Click Close after the installation completes.

Install the CA SAM Import and Export Service

Install the CA SAM Import and Export Service component on the CA SAM server if you are implementing CA APM and CA SAM.

Note: You do not need to install the CA SAM Import and Export Service if you are not implementing CA SAM as your software asset management system.

Important! Microsoft .NET Framework 4.0 must be installed on the CA SAM server before you install the CA SAM Import and Export Service.

Follow these steps:

1. Log in to the CA SAM server.
2. Navigate to the SAMImportExportSetup folder on the CA APM installation media. Copy the folder and all of its contents to a local folder on the CA SAM server.
3. In the SAMImportExportSetup folder on the CA SAM server, double-click CAITAMSAMImportExportServiceInstaller.msi.

   A prompt for the installation root path appears.
4. Enter the ITAM root path for installing the CA SAM Import and Export Service component.

   The following example shows the recommended path.

   Example:

   C:\Program Files\CA\ITAM

   You have completed installing the CA SAM Import and Export Service.

Configure the CA SAM Import and Export Service

The CA SAM Import and Export Service exports discovered hardware data to CA APM. This service receives ownership data exports from CA APM and updates asset information in CA SAM. This service also receives the automatic data synchronization exports (Company, Location, Cost Center, Division, and Contact) from CA APM and updates the information in CA SAM.

Follow these steps:

1. Log in to the CA SAM server.
2. Navigate to the following location:

   [ITAM Root Path]\ITAM\SAMImportExportService
3. Open the web.config file in a text editor.
4. Edit the import folder path by performing the following steps.
   a. Locate the following statement:

      <add key="ImportFolderPath" value="*[import folder path]*"/>
   b. Replace [import folder path] with the path of the external folder under the data exchange folder. The data exchange folder is located under the CA SAM install folder.

      Example:

      C:\Program Files (x86)\ca_sam\app\uploads\prod\data_exchange\external

5. Edit the export folder path by performing the following steps.

   a. Locate the following statement:

      `<add key="ExportFolderPath" value="[export folder path]"/>`

   b. Replace [export folder path] with the path of the "in" folder under the external folder. The external folder is under the data exchange folder, which is located under the CA SAM install folder.

      Example:

      `C:\Program Files (x86)\ca_sam\app\uploads\prod\data_exchange\external\in`

6. Save the web.config file.

7. Navigate to the following location:

   `[ITAM Root Path]\ITAM\SAMImportExportService\data_exchange`

8. Configure the device export by copying one of the following files to the export folder path:

   - CA_SAM_Device_Export_SQL.xml (for a SQL Server database)
   - CA_SAM_Device_Export_ORA.xml (for an Oracle database)

   Example:

   `C:\Program Files (x86)\ca_sam\app\uploads\prod\data_exchange\external\in`

9. Create a cron job to use the external folder by performing the following steps.

   a. Log in to CA SAM as the Administrator.

   b. Click Admin, Configuration, Cron jobs.

   c. Click the New record icon (*) in the Cron jobs toolbar.

   d. Specify the following information:

      Function Name

      Select data_exchange_external.

      Description

      Enter the following description: CA Data Coordination Service Tasks.

      Interval (minutes)

      Enter a value for the import and export time interval (for example, 5).

   e. Click Save.

      The dialog closes.

10. Select the XML file for the cron job.
    a. Select Exchange, Data Exchange, Exchange directory.
    b. Select external in the Exchange Directory field.
    c. Select XML files in the Show field.
    d. Click Browse, then locate and select one of the following XML files:
        - CA_SAM_Device Export_SQL.xml (for a SQL Server database)
        - CA_SAM_Device Export_ORA.xml (for an Oracle database)
    e. Click Upload File.
    f. Click the Start icon for the data_exchange cron job.

       The Start cron job dialog appears.
    g. Click Start cron job.

       The dialog closes.

    The configuration of the CA SAM Import and Export Service is complete.

Configure the CA APM Event Service for CA SAM

Configure the CA APM Event Service by validating or editing the parameters on the CA APM Administration tab.

Follow these steps:

1. Log in to CA APM on the web server as the administrator.
2. Navigate to Administration, System Configuration, Event Service page.
3. Click Show Advanced Options.

   The parameters that apply to CA SAM appear.
4. Validate or edit the values in the following parameters:

   Interval between Event Occurrence check (in milliseconds)

   The amount of time, in milliseconds, that CA APM waits between database checks for field changes related to defined events.

   If SAM capabilities are enabled, verify that this parameter is set to 30000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.

   Default (without CA SAM implementation): 3600000 (1 hour)

   Default (with CA SAM implementation): 30000 (30 seconds)

Interval between triggering events check (in milliseconds)

Amount of time, in milliseconds, that CA APM waits between database checks for triggered events that need to be sent to the workflow provider.

If SAM capabilities are enabled, verify that this parameter is set to 60000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.

Default (without CA SAM implementation): 3600000 (1 hour)

Default (with CA SAM implementation): 60000 (60 seconds)

Interval between triggered events status update (in milliseconds)

The amount of time, in milliseconds, that CA APM waits between updates to the status of triggered events that were sent to the workflow provider.

If SAM capabilities are enabled, verify that this parameter is set to 60000. If SAM capabilities are not enabled, verify that this value matches the setting in the Event Service configuration file.

Default (without CA SAM implementation): 3600000 (1 hour)

Default (with CA SAM implementation): 60000 (60 seconds)

Interval between asset contact update (in milliseconds)

The amount of time, in milliseconds, that CA APM waits between updates to asset contacts in the CA CMDB.

Default: 43200000 (12 hours)

CA SAM Status Update Frequency

The frequency for updating the status of CA SAM import jobs in the MDB (in milliseconds).

Default: 120000 (120 seconds)

On Demand Max Threads

The maximum number of threads for processing the data synchronization between CA APM and CA SAM. The default (zero) indicates that the system creates the required number of threads, depending on the system hardware configuration. Any value other than the default value uses the same number of threads, regardless of the system configuration.

Default: 0

CA SAM Events Notification Email

The CA APM administrator email address for receiving notifications about the CA SAM data synchronization.

Authorization Token

The token that establishes communication between the CA APM Event Service and the CA SAM Import and Export Service. This value must match the CA SAM Import and Export Service configuration setting.

Note: If you change this value, you must update the value of the Authorization Token for the CA SAM Import and Export Service on the CA SAM server to match this value.

Query Top

The number of triggered events that are processed at one time.

Example: This value is set to 1000 and 1500 events are triggered. The first processing pass processes the first 1000 records, and the next processing pass processes the remaining 500.

Default: 1000

Configure the SAM Import Driver

Configure the SAM Import Driver by validating or editing the parameters on the CA APM Administration tab.

Follow these steps:

1. Log in to CA APM on the web server as the administrator.
2. Navigate to Administration, System Configuration, SAM Import Driver page.
3. Validate or edit the values in the following parameters:

Server

The name of the server where the CA SAM Import Driver component is installed.

Username

The user name that is required for adding, changing, or deleting records with the Data Importer.

ITAM Root Path

The path to the root location where the product is installed.

File Path

The path to the root location where CA SAM export files are imported.

Example: *[ITAM Root Path]*\ITAM\Import Driver\Input

Import Processor Executable Path

The path to the Data Importer Processor executable file (ImportProcessor.exe).

Example: *[ITAM Root Path]*\ITAM\Import Processor\ImportProcessor.exe

Schedule the Windows Task for the Hardware Import

Use the Windows Task Scheduler to schedule a task to import into CA APM the discovered hardware data from CA SAM. The following procedure schedules the import to run once every day.

Note: While this procedure describes the use of the Windows Task Scheduler, you can also use another task scheduler or process orchestration tool.

Follow these steps for Windows Server 2008:

1. From the Start menu on the CA APM application server, open the Windows Task Scheduler.

   For example, on Windows Server 2008, go to Control Panel, System and Security, Administrative Tools, Schedule Tasks.
2. Click Create Task.
3. On the General tab, enter a name for the task.
4. Select the check box for “Run whether user is logged in or not”.
5. Navigate to the Actions tab and click New.
6. In the Action field, select Start a program.
7. In the Program/script field, browse to locate the Import Driver Program folder, select the ImportDriver.exe file, and click OK.
8. Navigate to the Triggers tab and click New.
9. In the Settings field, select Daily.
10. In the Start field, select 12:00:00 AM.
11. Select Recur every 1 day and click OK.
12. On the Create Task dialog, click OK.

    You have completed scheduling the Windows task to import discovered hardware data.

Start the CA APM Event Service

If you are upgrading from a previous CA APM release, you start the CA APM Event Service to complete the implementation of CA SAM with CA APM:

Follow these steps:

1. From the Start menu on the CA APM application server, open the Control Panel, Administrative Tools, Services.
2. Locate the entry for the CA Asset Portfolio Management – Event Service.
3. Right-click the service and select Start.

   The service is started.

Enable Software Asset Management Capabilities

After you install and configure all CA APM components, you then enable the software asset management capabilities.

If you currently have an integration between CA APM and CA Software Compliance Manager (CA SCM), uninstall CA SCM before you enable software asset management capabilities. For information about uninstalling CA SCM, see How to Uninstall CA Software Compliance Manager (see page 145). For more information about how and when to uninstall CA SCM, contact your CA Services representative.

Note: If you enabled software asset management capabilities in a previous release and you are now upgrading, skip the following steps. However, update the web.config configuration file on the CA APM web server to refer to the CA SAM section of the common home page. Update the following statement:

```
<add key="CASAMWebClientUrl" value="http://CA_SAM_server_name/prod" />
```

Example:

```
<add key="CASAMWebClientUrl" value="http://itamsam/prod" />
```

Follow these steps:

1. Log in to CA APM on the web server as the Administrator.
2. Navigate to Administration, System Configuration, Software Asset Management.

3. Complete the requested information. The following fields require explanation:

CA SAM Web Client URL

Specifies the URL for the CA SAM home page.

Note: You can copy the web client URL from the CA SAM home page after you log in.

CA SAM Import Export Webservice URL

Specifies the URL for the CA SAM web service. Use the following format:

`http://[CA SAM System Name]:[Port Number]/SAMImportExportService/Service.svc`

- Replace [CA SAM System Name] with the name of the CA SAM server.
- Replace [Port Number] with the port number where the CA SAM Import and Export Service is hosted.

Enable SAM Capabilities

Specifies that software asset management capabilities are enabled. If you previously had CA SCM fields on the CA APM user interface, they are removed after you select this check box.

CA SAM Web Service WSDL URL

The URL for the CA SAM Web Service Definition Language (WSDL). This URL is used to access the CA SAM web service. Use the following format:

`http://[CA SAM System Name]:[Port Number]/prod/soap/dyn_server.php`

- Replace [CA SAM System Name] with the name of the CA SAM server.
- Replace [Port Number] with the port number where the CA SAM Web Service is hosted.

CA SAM Web Service Login

Login name for the CA SAM web service.

Note: Verify that this login name and the CA SAM Web Service Password match the login name and password in the config_soap.inc file. This file is found in the following CA SAM installation folder path:

`app\includes\prod\st\config_soap.inc`

Important! The default content of the config_soap.inc file is commented. Remove the comment delimiters (/* */) and configure the login name and password.

CA SAM Web Service Password

Login password for the CA SAM web service.

CA SAM SSO Encryption Algorithm

Specifies the encryption algorithm to be used for single sign-on access to CA SAM from the CA IT Asset Manager common home page.

This entry must match the entry in CA SAM System Configuration for the security_auth_token_cipher field.

Note: For more information about CA SAM single sign-on, see the description of single sign-on in the *CA Software Asset Manager Administration Manual.*

CA SAM SSO Authentication Mechanism

Specifies the mechanism to be used for logging in to CA SAM.

This entry must match the entry in CA SAM System Configuration for the security_auth_method field.

Note: We recommend that you select auth_token_password for this mechanism. The auth_token mechanism disables the login for other CA SAM users.

CA SAM SSO Field to Authenticate User

Specifies the type of unique identifier (import ID or email address) that is used to authenticate the user.

This entry must match the entry in CA SAM System Configuration for the security_auth_token_user_identifier field.

CA SAM SSO Secret Key

Specifies the key that CA APM and CA SAM share and that is used to encrypt and decrypt the user authentication. This key ensures that CA APM users who do not have the proper authentication cannot access CA SAM.

This entry must match the entry in CA SAM System Configuration for the security_auth_token_key field.

4. Click Save.
5. Restart the Apache Tomcat Common Asset Viewer service.

   Note: Also restart the Apache Tomcat Common Asset Viewer service if you change the entries in any of the following fields at a later time:

   - CA SAM Web Service WSDL URL
   - CA SAM Web Service Login
   - CA SAM Web Service Password
6. Restart Internet Information Services (IIS) on the CA APM web servers and application servers by executing the iisreset command.

   Software asset management capabilities are enabled, and CA SCM fields are removed from the CA APM user interface.

The Load Data button is enabled if CA APM data exists (for example, if you had an existing CA APM 12.6 installation and you are upgrading). You can then load existing CA APM data for selected objects into CA SAM. For information about loading data, see Load CA APM Data into CA SAM (see page 139). This button is not enabled if you are performing a new installation of CA APM. You do not have existing data with a new installation.

Common Home Page Single Sign-On

When the CA SAM implementation is complete, the CA IT Asset Manager common home page displays Hardware and Software Asset Management dashboards. These dashboards contain links that open pages in CA APM and CA SAM. After you log in to CA APM and open the common home page, you can access CA SAM pages without logging in to CA SAM.

To implement the single sign-on, verify that the following steps are completed:

- The user ID in CA APM exists as a user ID in CA SAM, also.
- The user email address and Import ID in CA SAM match the user email address and Contact ID in CA APM.
- The CA SAM user is authorized to perform CA SAM functions.
  a. Access the CA SAM user details page by selecting Organization, User, and then editing an existing user record or creating a user record.
  b. Select the check box for CA Software Asset Manager authorization.

Load CA APM Data into CA SAM

After you enable software asset management capabilities in CA APM, you can load existing CA APM data for selected objects into CA SAM. This data load allows you to synchronize the data so that objects that match in CA APM and CA SAM have the same data values. The CA APM data that you can load includes the following objects:

- Location
- Division
- Company

- Cost Center
- Contact

If you had a previous installation of CA APM, you have existing CA APM data for these objects. If you are performing a new installation of CA APM, you do not have any existing data.

Note: Before you load CA APM data into CA SAM, verify that your CA APM data meets CA SAM requirements. These requirements are defined in Field Requirements for Automatic Data Synchronization.

Follow these steps:

1. On the Administration, System Configuration, Software Asset Management page, verify that the Load Data button is enabled.

   Note: The Load Data button is enabled if CA APM data exists (for example, if you had an existing CA APM 12.6 installation and you are upgrading).

2. Click Load Data.

   The data load copies the Location, Division, Company, Cost Center, and Contact object values to CA SAM. A status table displays the progress of the data load.

   If some of the objects fail to synchronize with CA SAM, the error records are written to a log file. You can view this log file by clicking the Get Error Records button. The Get Error Records button is available only after you enable SAM capabilities.

3. Click Get Error Records to verify if any data synchronization errors occurred.

   You are prompted to open or save a CSV file. If errors exist in the CSV file, the errors are grouped by object in the following order:

   - Location
   - Division
   - Company
   - Cost Center
   - Contact

4. Review the errors and explanations in the CSV file and correct the CA APM object data.

   The corrected objects are synchronized with CA SAM during the next data synchronization.

Data Management Recommendations

The recommendations in this section help you manage your data when CA APM is implemented with CA SAM.

Manual Data Synchronization

Data must be synchronized between CA APM and CA SAM to maintain the integrity of the data and of the asset management process. Data synchronization ensures that objects that are the same in both CA APM and CA SAM contain the same data values.

When you create or update the Country and Region objects in CA APM or CA SAM, synchronize the objects manually. For example, if you create a Country object in CA SAM, manually create the same object in CA APM. If you update a Region object in CA APM, manually update that object in CA SAM.

Manual Data Synchronization Rules

To ensure that data is synchronized correctly, use the following rules when you create or update the Country and Region objects:

- Country–The CA APM abbreviation for a country must match the CA SAM record import ID for the same country.
- Region–The CA APM name for a region must match the CA SAM record import ID for the same region.

Cost Center Data Management

The data synchronization between CA APM and CA SAM ensures the integrity of the data and of the asset management process. This synchronization occurs automatically for the following objects:

- Company
- Location
- Cost Center
- Division
- Contact

Note: These objects use the same labels in CA APM and CA SAM, except Contact. In CA SAM, the Contact object is labeled "User".

When you create, update, or delete the Contact, Company, Location, and Division objects in CA APM, the objects are automatically synchronized in CA SAM. The CA SAM Administrator must designate Contact, Company, Location, and Division as read-only in CA SAM. This action prevents CA SAM users from changing these objects, which will be overwritten when the next data synchronization occurs. However, the Administrator cannot designate the Cost Center object as read-only in CA SAM because the Cost Center reporting hierarchy must be administered in CA SAM.

Recommended Guidelines for Cost Center Data Management

To facilitate Cost Center data management, we recommend that you use the following guidelines:

- Add permissions to manage the Cost Center object to an Administrator role in CA SAM. Other user roles are not able to access the Cost Center object.
- Use CA APM when you perform the following actions:
  - Insert or delete Cost Centers.
  - Update Cost Center name or description.

  Important! If you change the Cost Center name or description in CA SAM, the changes are overwritten after the next data synchronization.
- Use CA SAM when you perform the following actions:
  - Administer Cost Center reporting hierarchy.
  - Assign a Cost Center to a country.

Inventory Units of Measurement

CA SAM sends hardware discovery data to CA APM to help with hardware asset management. CA APM requires specific units of measurement for the following hardware inventory items that are sent from CA SAM:

- Total Disk Space: Gigabytes (GB)
- Total Memory: Megabytes (MB)
- Processor (CPU) Speed: Megahertz (MHz)

When you load and manage hardware inventory data for these items in CA SAM, verify that the CA SAM data uses these units of measurement.

Field Requirements for Automatic Data Synchronization

Automatic data synchronization copies the CA APM data for the Company, Location, Cost Center, Division, and Contact objects to the corresponding objects in CA SAM. To ensure a successful synchronization, follow the field requirement guidelines for the objects in the following subsections.

Contact

Some of the fields for the Contact object are optional in CA APM but required in CA SAM. These fields are summarized in the following table. Verify that all fields that are required in CA SAM contain data in CA APM.

CA APM Field	Required in CA APM?	Required in CA SAM?
User ID/User Name	No	Yes
Cost Center	No	Yes
Last Name	Yes	Yes
First Name	No	Yes

Company

CA SAM allows you to report compliance for hierarchical groupings (Division, Company, and Cost Center). To report on Divisions, CA SAM requires Division details for the Company object. Verify that the CA APM Company object has Division details to ensure a successful data synchronization.

Note: To enter Division details for a company in CA APM, you first create divisions in Directory, List Management, Company Lists, Division. Then when you create or update a company on the Company Details page, select a Company Type of Internal. The Division text box appears and you can select a division for the company.

Cost Center

CA SAM allows you to report compliance for hierarchical groups (Division, Company, and Cost Center). To report on Companies, CA SAM requires Company information for the Cost Center object. Verify that the CA APM Cost Center object has Company details to ensure a successful data synchronization.

Assets with Undefined Operating Systems

Discovery data that CA APM receives can contain operating system names that are not defined in CA APM. When this situation occurs, CA APM assigns an operating system value of Undefined to the corresponding asset. CA APM displays the Undefined value in the Operating System field on the Asset Details page.

You can view the original discovered names of the Undefined operating systems, and you can add those names to the CA APM operating system names. You can also update the assets that have Undefined operating systems to include the new names.

Note: CA APM can receive data with undefined operating systems from any discovery source (including CA SAM).

Follow these steps to view the original names of Undefined operating systems:

1. Log in to CA APM as the administrator.
2. Navigate to Administration, Reconciliation Management, Reconciliation Message Search.

   A list of Reconciliation messages displays.
3. Locate the messages that identify the missing operating systems.

   Note: You can search on this page for "Missing Operating System" in the message text.

   The messages include the original discovered names.

Follow these steps to update assets with Undefined operating systems:

1. Navigate to Directory, List Management, Operating System and add the missing operating system names to the CA APM names.
2. Update an individual asset with an Undefined operating system by using the following steps:
   a. Navigate to the Asset Details page for an asset with an Undefined operating system.
   b. Click the Select New icon in the Operating System field and select the new name.
3. Update multiple assets with Undefined operating systems by using the following steps:
   a. Navigate to Administration, Reconciliation Management.
   b. Click the reconciliation rule name.

      The Reconciliation Rule Details page appears for the selected rule.

c. Verify that Monitor Asset Updates is selected.

d. In the Update Options area, select Operating System and Last Run Date.

e. Click Save.

When CA APM receives new discovery data for assets with Undefined operating systems, CA APM updates the operating systems with the new names that you entered.

How to Uninstall CA Software Compliance Manager

To enable SAM capabilities when CA APM is integrated with CA Software Compliance Manager (CA SCM), uninstall CA SCM.

Note: Verify that all users have logged out from CA SCM. Any user who does not log out from the product before the uninstallation begins receives an error when attempting to complete a task.

Follow these steps to uninstall CA SCM 12.0:

1. Log in to the computer on which you installed CA SCM 12.0.
2. Uninstall the CA SCM Release 12.0 cumulative patches, if any, through the Control Panel, Add/Remove Programs.
3. Log in to the CA APM application server where you installed CA APM Release 12.9.
4. Navigate to the folder where you installed CA APM Release 12.9.
5. Copy the SWCM12.0Uninstall folder and all of its contents to a temporary location on each computer (except the database server) where you installed CA SCM 12.0.

   Example of temporary location:

   `C:\Windows\Temp`
6. Navigate to the Uninstall folder in the temporary location on the CA SCM 12.0 computer.
7. Start the uninstallation by double-clicking the SWCM_Uninstall.bat file.
8. Follow the on-screen instructions in the uninstallation process.

   The uninstallation runs and successfully removes all installed CA SCM 12.0 components, except CA Business Intelligence BusinessObjects Enterprise, CA EEM, CA MDB, and the Content Import Client.

Follow these steps to uninstall CA SCM 12.6:

Note: Complete these steps on each computer (except the database server) on which you installed CA SCM 12.6.

1. Log in to the computer on which you installed CA SCM 12.6.
2. Uninstall the CA SCM Release 12.6 cumulative patches, if any, through the Control Panel, Add/Remove Programs.
3. Navigate to the Uninstall folder where CA SCM 12.6 is installed.

   Example:

   ```
   C:\Program Files\CA\SWCM\Uninstall
   ```

4. Start the uninstallation by double-clicking the SWCM_Uninstall.bat file.
5. Follow the on-screen instructions in the uninstallation process.

   The uninstallation runs and successfully removes all installed CA SCM 12.6 components, except CA Business Intelligence BusinessObjects Enterprise, CA EEM, CA MDB, and the Content Import Client.

Chapter 8: Troubleshooting

This section contains the following topics:

Installation Does Not Start or Displays Server Not Found Error

Valid on all supported operating environments.

Symptom:

When starting the CA APM installation, the installation does not start or you receive a Server Not Found error.

Solution:

Restart the UtilDev Web Server Pro Windows service.

Tenancy Management Page Cannot Be Displayed Browser Error Appears

Symptom:

The following browser error message appears when I click Administration, Tenancy Management:

```
Page cannot be displayed.
```

Solution:

Verify that the CA CASM service is started (see page 22).

Tenancy Management Page Does Not Appear

Symptom:

When I click the Administration tab, I do not see a Tenancy Management option.

Solution:

Your CA APM administrator has not assigned you to a role in which Tenancy Administration Access is enabled. If you need access to Tenancy Management, contact your CA APM administrator.

Web Servers Named with Underscore Characters

Valid on all supported operating environments.

Symptom:

Using underscore characters in web server host names may cause problems when logging in to the product or when using CA EEM for user configuration.

Solution:

If you are using a virtual or ghosted system, configure a new host name by creating another image without the underscore character. For a production system, add a new host name to your internal Domain Name System (DNS) so that the product can be accessed with a different URL.

Log In Fails with a User Name Containing Extended Characters

Symptom:

When using CA EEM with Single DB Login authentication, I cannot log in to the CA APM web interface.

Solution:

Select a User Name that does not contain extended characters (that is, Japanese or German characters).

WCF Services Fail when IIS 7 is Installed on Windows 2008

Valid on Windows 2008 operating environments.

Symptom:

When I have Microsoft Internet Information Services (IIS) 7 installed on Windows 2008, the WCF Services do not work. CA APM uses a WCF Service to implement the web services function.

Solution:

This problem occurs because the service file types are mapped incorrectly or the Windows components, including IIS 7, were installed in an incorrect order. To correct the problem, verify and change (if necessary) the IIS settings. Microsoft provides information and solutions for the problem.

Complete the following steps to resolve the problem:

1. In a web browser, open the Microsoft website (http://www.microsoft.com) and search for "IIS Hosted Service Fails".
2. Follow the instructions in the article.

Missing Operating System Message Appears in Message Queue

Symptom:

I receive one of the following error messages in the message queue during the Reconciliation Engine processing of normalization rules:

- The following discovered operating systems are missing from the Public Operating System list:

  Missing Operating System: *operating system name*

- The following discovered operating systems are missing from the Operating System list and must be added to the Public Operating System list or the list for tenant: *tenant name*

  Missing Operating System: *operating system name*

Note: The Reconciliation Engine writes messages to the message queue in the database. Set the Engine Debug Level in the Hardware Reconciliation Engine Configuration Settings to Fatal (or a higher level of detail) for these error messages to appear in the message queue. For more information about the message queue and the configuration settings, see the *CA APM Administration Guide*.

Solution:

The normalization rules apply to all tenants and public data and can be used across tenants. If an operating system value assigned through the normalization list does not exist for a tenant, the Reconciliation Engine produces an error message to inform you that the operating system must be added for that tenant or as public data.

Note: For more information about normalization rules, see the *CA APM Administration Guide*.

If one or two operating systems are missing, you can resolve the problem by adding the operating systems manually to the normalization rules. For information about how to define operating system normalization rules, see the *CA APM Administration Guide*.

If numerous operating systems are missing, complete the following steps to resolve the problem:

1. Log in to CA APM and click Administration, Reconciliation Management.
2. On the left, click Reconciliation Message Search.

   The message queue displays reconciliation log messages in the Search Results.
3. Search to find the missing operating system normalization rule error messages.

   The message queue displays all missing operating system normalization rule error messages.
4. Verify that the system administrator email address in the product is correct and click Export to CSV.

   The operating systems that are missing are exported to a CSV file. The system administrator receives an email message with a link to the CSV file.
5. Edit the content of the CSV file to prepare the file for the Data Importer. For example, you can remove duplicate operating systems or extraneous words from the file.

   Note: For more information about using the Data Importer, see the *Administration Guide*.
6. Log in to the CA APM, click Administration, Data Importer, and select the tenant or public data that is missing the operating systems.
7. Import the CSV file.

   The missing operating systems are imported into the CA MDB and are available for use during Reconciliation Engine normalization processing.