CA Asset Portfolio Management

Administration 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:

Audience

This guide is intended for the CA APM administrator, the person who has overall responsibility for the administration of the product. The purpose of this guide is to help you prepare the product for the daily management of assets by users.

This guide assumes that the product has been installed, based on the information in the *Implementation Guide*.

Administration

The overall administration of CA APM involves setting up security, configuring the user interface, managing hardware reconciliation, and optionally changing configuration settings for product components. The product administration is flexible and you can complete the following administration tasks in any order that you want.

After you complete the following tasks, provide the CA APM URL and login credentials to all users so that they can log in to the product.

Security

You define security to control user access to the product and features. For example, you can provide one user with access to models and assets, and another user with access to legal documents.

Note: For more information, see Security (see page 11).

User Interface Configuration

You configure the user interface to simplify how users enter, manage, and search for data. In addition, you secure and protect users from performing unauthorized tasks and ensure that you conform to your IT asset management practices. For example, you can globally hide the Contact page from all CA APM users. However, there are some users who must be able to see and update contact information. Therefore, you make the Contact page appear for those users. User interface configuration is flexible, and you can configure almost all aspects of the user interface.

Note: For more information, see How to Configure the User Interface.

Hardware Reconciliation

You use hardware reconciliation to match *discovered assets* to their corresponding *owned assets* from different logical repositories and manage your assets. You can identify unauthorized, missing, under-utilized, and over-utilized assets, which helps you to optimize your hardware asset base.

Note: For more information, see Hardware Reconciliation.

Product Components

You can change the product component configurations that were set up during the product installation. For example, you can change the listening port for Oracle. You can also add components to additional servers to maintain product performance and enable product scalability. For example, you can add a Hardware Reconciliation Engine on an additional server. The configuration is flexible, and you can change many component settings.

Note: For more information, see Configure a Product Component (see page 127) and Add Component Servers (see page 150).

Log In to CA APM

After the product is installed, your implementer verifies that all services are started and starts the web interface to verify that CA APM is ready to use. The implementer provides you with the URL and credentials to log in to the product. You can then prepare the product for users to manage assets.

By default, the login credentials (username and password) for the default System Administrator user are uapmadmin. You can change the password to meet your requirements by changing the settings for the CA EEM component.

Note: The default password can also be changed during the installation process.

Chapter 2: Maintaining Security

This section contains the following topics:

Security

Before you allow user access to CA APM, set up security to control access to the product, protect your repository from unauthorized or inaccurate changes, and make necessary data available to users. For example, you can provide one user with access to models and assets, and another user with access to legal documents.

Setting up security involves the following tasks:

1. Users (see page 12). Define the users who can access the product.
2. User Roles (see page 15). Define groups of users who perform similar tasks.
3. Authentication (see page 23). Define how users are authenticated when they log in.
4. Searches (see page 25). Define which users can use searches.
5. Configuration (see page 29). Protect users from performing unauthorized tasks.

One or more system administrators perform these security tasks in CA APM. A system administrator with the user ID *uapmadmin* acts as a global system administrator, with complete control over all security aspects of the product.

You enforce security across the enterprise by using the web interface. Minimal database skills are required to perform these tasks.

Users

You establish user security when you add new users to the product and assign a user ID and password. If a user does not have a valid user ID and password, they cannot log in. For each person, a user record is established, and the record is associated with a contact in the ca_contact table.

You can add users to the product in the following ways:

1. Import them (see page 12).
2. Manually define them (see page 13).

When manually defining users, you can immediately authorize them to use the product. However, when you import users, import them first, and then you can authorize them (see page 14).

Note: When you define a user manually, a corresponding CA EEM user is also created. CA EEM verifies the user name and password when the user logs in to CA APM.

After you define all CA APM users, assign each user to a *user role* and assign the entire role access rights to determine what they see and can access when they log in.

Best Practices (Users and Roles)

Use the following best practices to effectively manage users and roles:

- A user must have a valid user ID and password, and be authorized, to log in.
- Remove a user from a role before assigning a new role to the user.

  Note: The product does not allow you to assign a user to more than one role.
- Verify that there are no users assigned to a role before deleting the role.
- Delete users before deleting a role.

Import and Synchronize Users

Important! Verify that the user completing this task belongs to a role in which user management access is enabled (see page 16).

You can import a list of users from an external user store such as an active directory through CA EEM, and synchronize them to be saved as contacts in CA APM. Importing users helps you to save time when defining your users, and helps ensure the accuracy of the user information. After you import and save the users, authorize them to access the product.

To import and synchronize users

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.
3. Click LDAP Data Import and Sync.

   The LDAP Data Import and Sync page appears.
4. If multi-tenancy is enabled, select a tenant from the drop-down list.
5. Click Start LDAP Data Import and Sync.

   The import process begins and users are imported from the external store. If multi-tenancy is enabled, users are imported for the selected tenant as contacts into the ca_contact table. You can then authorize the imported users to access the product (see page 14).

Important! The LDAP Data Import and Sync works for user names that begin with a letter or number. User names that begin with a special character are not imported.

Define a User

Important! Verify that the user completing this task belongs to a role in which user management access is enabled (see page 16).

You define all users of CA APM and provide them with access to the product. After you define a user, assign a role to the user (see page 19).

To define a user

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.
3. Click New User.

   The New User page appears.
4. Enter the information for the new user and the contact-related information.
5. (Optional) Specify if you want to authorize the user to access to the product.
6. Click Save.

   The user is defined.

Authorize a User

Important! Verify that the user completing this task belongs to a role in which user management access is enabled (see page 16).

You can authorize a user so they can log in and use the product. Before you can authorize a user, save the user as a contact.

To authorize a user

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.
3. Click Authorize Users.

   The Authorize Users page appears.
4. Search to find the list of available users.
5. Select the user you want to authorize and click OK.

   The user appears in the Authorized Users list.
6. Click the Edit icon next to the user name.
7. (Optional) Select a contact to assign a user with contact details.

   Note: If you do not select a contact, a new contact is created for the user.
8. (Optional) Select a role to assign to the user.
9. Click Authorize.

   The selected user is authorized to log in to the product.

Deny a User Access

Important! Verify that the user completing this task belongs to a role in which user management access is enabled (see page 16).

You can deny a user access and prevent them from logging in to the product. For example, you hire a new asset technician and want to prevent them from using the product until they have received proper training. When you deny a user access, the contact information for the user is not deleted from the product.

To deny a user access

1. Click Administration, User/Role Management.
2. On the left, expand the User Management menu.

3. Click Authorize Users.

   The Authorize Users page appears.

4. Select the user for which you want to deny access from the Authorized Users list.

5. Click De-Authorize.

   The user is prevented from logging in to the product.

User Roles

A *user role* is the primary record that controls security and user interface navigation in the product. Each role defines a focused view of the product by exposing only the functionality necessary for users to perform the tasks that are assigned to their business roles. The default role for a user and the associated user interface configuration determine the data and functions that are available to the user. A user can belong to only a single role.

Define 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. Group the users with the same job function and assign them the corresponding role. Role assignment prevents the users from performing unauthorized tasks, such as adding or deleting data. For example, users in an Administrator role need full access to all records, while users in an Asset Technician role need limited access to fewer records.

Note: The product contains predefined System Administrator and user roles that you can use as the basis for user management.

You can perform several tasks to set up and manage user roles:

- Define a role (see page 16).
- Assign a role to a user (see page 19).
- Remove a user from a role (see page 20).
- Update a role (see page 21).
- Delete a role (see page 22).
- Assign a configuration to a role (see page 21).

Predefined Roles

The product provides a System Administrator role, which has complete control and access to all objects and tenant data. This role is associated with the System Administrator contact and cannot be deleted. A user in this role can define, update, and delete objects, in addition to defining and updating more roles to meet your business requirements. You cannot assign a configuration to the System Administrator role.

The product also provides the following predefined user roles to help you manage users:

- CA APM Asset Technician–Provides access to the data and functions that are required for working with asset information only.
- CA APM Contract Manager–Provides access to the data and functions that are required for working with legal documents and the contract management process only.
- CA APM Default User–Provides read-only access to a limited view of the product. This role can view most of the data in the product. However, this role cannot modify the product data.
- CA APM Fulfiller–Provides access to the data and functions that are required for asset fulfillment tasks only.
- CA APM Receiving–Provides access to the data and functions that are required for updating assets that are received from a fulfillment process only.

Each predefined user role has associated configurations, which provide access to the data that is required to complete the particular function. You can modify the configurations that are associated with each predefined role. The predefined roles are available only after a new installation.

Define a User Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled (see page 16).

You can define customized user roles to meet your site-specific business requirements. For example, you can define one role with access to reconciliation management, and another with access to asset fulfillment.

To define a user role

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click New Role.
4. Enter the information for the role.

   User Management Access

   Select this check box so a user assigned to the role can access the user management functionality (Administration, User/Role Management, User Management). The User/Role Management subtab is available only when the role has access to the user management functionality, the role management functionality, or both.

Role Management Access

Select this check box so a user assigned to the role can access the role management functionality (Administration, User/Role Management, Role Management). The User/Role Management subtab is available only when the role has access to the user management functionality, the role management functionality, or both.

System Configuration Access

Select this check box so a user assigned to the role can access the system configuration functionality (Administration, System Configuration).

Web Services Access

Select this check box so a user assigned to the role can access the CA APM web services documentation and WSDL (Administration, Web Services). If this check box is not selected and a user in the role attempts to access the web services from an external client application, the user receives a login error.

Filter Management Access

Select this check box so a user assigned to the role can access the filter management functionality (Administration, Filter Management).

Other Information Configuration Access

Select this check box so a user assigned to the role can access the Other Information Configuration functionality. This function allows the user to access additional related information for selected objects. The user can access this additional information by selecting menu items under Relationships on the left side of the page.

Data Importer User Access

Select this check box so a user assigned to the role can access the Data Importer functionality (Administration, Data Importer) with user permissions. Users can create imports and can modify or delete their own imports. Users can also view any import that was created by another user.

Data Importer Admin Access

Select this check box so a user assigned to the role can access the Data Importer functionality (Administration, Data Importer) with administrator permissions. Administrators can create imports and can modify or delete any import that was created by any user.

Reconciliation Management Access

Select this check box so a user assigned to the role can access the reconciliation rules management functionality (Administration, Reconciliation Management).

Asset Fulfillment Access

Select this check box so a CA Service Catalog user assigned to the role can perform asset fulfillment using CA Service Catalog.

Note: For more information about asset fulfillment using CA Service Catalog, see the CA Service Catalog documentation.

Tenancy Admin Access

Select this check box so a user assigned to the role can access the multi-tenancy administration functionality to enable multi-tenancy, define tenants, define subtenants, and define tenant groups (Administration, Tenancy Management).

Normalization Access

Select this check box so a user assigned to the role can access the normalization rules management functionality (Directory, List Management, Normalization).

Mass Change Utilities Access

Select this check box so a user assigned to the role can access the Mass Change Utilities functionality. This function allows the user to change the asset family for a model and also to change the model for an asset.

5. (Optional) Specify the read/write permissions for tenants. Multi-tenancy expands the purpose of the role to control the tenant or tenant group that a user within the role can access. When multi-tenancy is enabled, the Tenant Information section includes Tenant Access Read and Tenant Access Write drop-down lists.

   Note: The Tenant Information section is visible only when multi-tenancy is enabled. For information about how to enable multi-tenancy, see the *Implementation Guide*. In addition, users associated with a tenant other than the service provider can only create or update objects associated with their own tenant. Only users associated with the service provider are permitted to create or update objects belonging to tenants other than their own.

   All Tenants

   Contains no tenant restrictions. A user in a role with this access can view any object in the database (including public objects). In addition, a user associated with the service provider can update or create objects associated with any tenant. When a service provider user with this access creates an object, the product requires the user to select the tenant of the new object.

   Contact's Tenant

   (Default value) Associates the role with the tenant of the contact. The product restricts a user in a role with this access to viewing, creating, and updating only those objects associated with their own tenant (and to view public objects). When a user with this access creates an object, the user cannot select a tenant. The tenant is automatically set to the tenant for the contact.

Contact's Tenant Group

Associates the role with the tenant group of the contact. The product restricts a user in a role with this access to viewing, creating, and updating only those objects associated with the tenants in their tenant group (and to view public objects). When a user with this access creates an object, the user can select any tenant belonging to the tenant group.

Single Tenant

Associates the role with a named tenant. When you select this option, select a specific tenant in either the Tenant Write or Tenant Read field. The product restricts a user in a role with this access to viewing, creating, and updating only those objects associated with the tenant you select (and to viewing public objects). When a user with this access creates an object, the user cannot select a tenant. The tenant is automatically set to the tenant you select.

Note: Only a service provider user can create or update data for a tenant other than their own. A tenant user in a role with single tenant access to another tenant is restricted to read access.

Tenant Group

Associates the role with a named tenant group. When you select this option, select a specific tenant group in either the Tenant Group Write or Tenant Group Read field. The product restricts a user in a role with this access to viewing only those objects that belong to any tenant in the tenant group. In addition, a user associated with the service provider can update or create objects associated with any tenant in the group. When a service provider user with this access creates an object, the product requires the user to select the tenant for the new object.

Update Public (check box)

Available only when you select All Tenants. Select this check box to authorize a user in the role to create or delete tenanted public data.

6. Click Save.

   The role is defined and you can assign users to the role.

Assign a Role to a User

Important! Verify that the user completing this task belongs to a role in which role management access is enabled (see page 16). In addition, if you do not assign a role to a user, the Administration tab is hidden from the user.

You can assign a role to a user to define a focused view of the product and determine what they see when they log in. For example, assign an administrator to the system configuration role. You can assign a user to only a single role. Save a user as a contact before you assign the user to a role.

Note: Remove a user from their previous role before assigning a new role to the user.

To assign a role to a user

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.

   The role details appear.
5. In the Role Contact area of the page, click Assign Contact.

   All users not assigned to a role appear.
6. Select the user for which you want to assign the role.
7. Click OK.
8. Click Save.

   The role is assigned to the user.

Remove a User from a Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled (see page 16).

You can restrict the access rights for a user by removing them from a role. For example, an administrator is transferred to a different department and you remove them from the system configuration role. Remove a user from a role before assigning them to another role, or if they are no longer a part of your site or organization.

To remove a user from a role

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.

   The role details appear.
5. Click the delete icon next to the user you want to remove from the role.
6. Click Save.

   The user is removed from the role.

Update a User Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled (see page 16).

At any time, you can update a user role to change what the user sees when they log in to the product. For example, the users in a particular role no longer perform tenancy management functions. In this situation, remove the tenancy management access for the role.

To update a user role

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.

   The role details appear.
5. Change the information for the role.
6. Click Save.

   The role is updated.

Assign a Configuration to a Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled (see page 16).

You can configure the user interface to simplify how users enter, manage, and search for data. When you assign a configuration to a role, you help ensure that any user assigned to the role sees the product as you have configured it for them.

Example: Assign a configuration to an asset manager

In this example, an asset manager must quickly view, and monitor the most important information that has been entered into the product for an asset. This information is used for reporting, cost analysis, and inventory control. The administrator configures the search results to display the asset name, model name, quantity, serial number, operating system, purchase order number, and cost center. The administrator saves the configuration and assigns it to the asset manager role. When an asset manager logs in to the product, the configuration for the asset manager role is selected and appears.

Note: For more information about configurations, see the chapter Configuring the User Interface (see page 29).

To assign a configuration to a role

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.

   The role details appear.
5. Click Role Configuration.
6. Click Select New.

   The list of saved configurations appears.
7. Select the configuration you want to assign to the role.
8. Click OK.
9. Click Save.

   The configuration is assigned to the role. Any user assigned to the role sees the configuration when they log in to the product.

Delete a User Role

Important! Verify that the user completing this task belongs to a role in which role management access is enabled (see page 16).

You can delete a role that is no longer active in your site or organization, or when the role functions are no longer required. You cannot delete the predefined System Administrator role (see page 15).

Note: Verify that there are no users assigned to the role before deleting a role. As a best practice, remove all users from a role before deleting a role.

To delete a user role

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.

   The role details appear.
5. Click Delete and confirm that you want to delete the role.
6. Click Save.

   The selected role is deleted.

Authentication

Authentication is the process of obtaining identification credentials from a user such as name and password to validate their credentials to verify that the user exists. If the credentials are valid, the user is authenticated. After a user is authenticated, the authorization process determines whether the user can log in to the product.

Note: CA APM uses CA EEM to process user authentication.

The following types of authentication are supported:

- Form Authentication (see page 23). A user is prompted for a user name and password to log in to the product.

  Note: Form authentication is the default authentication type.

- Windows Integrated Authentication (see page 24). A user already logged in to the Windows domain can access the product without having to provide additional login credentials.

Note: You can provide additional security by defining tab and menu configuration (see page 40) in the product to restrict the pages and tabs that a user can access.

More information:

Single Sign-On (see page 25)

Configure Form Authentication

Important! Verify that the user completing this task belongs to a role in which system configuration access is enabled (see page 16).

You can configure form authentication so a user is prompted for a user name and password when logging in.

To configure Form Authentication

1. Click Administration, System Configuration.
2. On the left, click EEM.
3. Select Form from the Authentication Type drop-down list.
4. Click Save.

   Form authentication is enabled.

Configure Windows Integrated Authentication

Important! Verify that the user completing this task belongs to a role in which system configuration access is enabled (see page 16).

You can configure Windows integrated authentication and reference the CA EEM server to the active directory used for authentication. With Windows integrated authentication enabled, a user already logged in to the Windows domain can access the product without having to provide any additional login credentials.

You can also configure Windows integrated authentication with CA EEM and CA SiteMinder. CA SiteMinder uses the active directory for authentication. For information about this configuration, see the CA EEM product documentation.

Note: For Windows integrated authentication to work, the CA EEM server, the Active Directory, and the client computer making the authentication request must belong to the same domain. In addition, when you create and authorize a user in the CA EEM local store with a user name that exists in the Active Directory, the corresponding Active Directory user is automatically authorized.

To configure Windows Integrated Authentication

1. On the computer where CA EEM is installed, configure the CA EEM server to reference your Active Directory or LDAP system.

   Note: For information about performing these functions, see the CA EEM product documentation.

2. In CA APM, click Administration, System Configuration.
3. On the left, click EEM.
4. Select Windows Integrated from the Authentication Type drop-down list.
5. Click Save.

   Windows integrated authentication is enabled.

Single Sign-On

Single sign-on is an authentication process where the user can enter one user ID and password and access a number of resources within the organization. Single sign-on eliminates the need to enter additional authentication credentials when switching from one solution to another.

Single sign-on lets users log in to the product automatically using Windows login information. After you add the user ID to any role, the product verifies the login credentials and displays the appropriate home page to the user.

Note: For single sign-on to work correctly, configure Windows user accounts as domain user accounts, and not as the local user accounts.

Search Security

Default searches let you find objects in the repository. For example, use the default searches to find assets, models, contacts, and so forth. The security for the default searches makes them available to all users and configurations. You can use these searches to create additional searches.

In contrast, you can apply security to the searches that you create to limit who can use the search. When you save a configured search, you can select specific user roles and configurations (restricted to administrators). By default, the security for the searches you create makes them available to all users and configurations. By applying unique security to your searches, you help ensure that certain users cannot view sensitive information that a search returns.

Consider the following information when applying security to searches:

- You can access all searches (default and user-defined searches) so that you can configure and troubleshoot searches for users.
- You can access all scheduled searches and exports so that you can configure and troubleshoot scheduled searches and exports for users.
- All users that are assigned to a role and configuration can access the default searches and the user-defined searches that are assigned to the role and configuration. However, the search results that users see for the default searches do not display information and fields that you hide and secure.
- When a default and user-defined search becomes invalid because of configuration changes, you may not need the search. You can delete any default and user-defined search in CA APM.

More information:

Troubleshooting Search Security (see page 26)

Troubleshooting Search Security

Troubleshooting tips related to search security help you when working with configured searches.

- Role Cannot Be Assigned to a Configured Search (see page 26)
- Configuration Cannot Be Assigned to a Configured Search (see page 27)

Role Cannot Be Assigned to a Configured Search

Valid on all supported operating environments.

Symptom:

When attempting to provide a role with access to a configured search, I receive an error similar to one of the following errors:

You cannot assign role <role name> to the search because the role cannot access the following field(s): <field name> on Asset Type <asset family>

You cannot assign role <role name> to the search because the role cannot access the Asset Type <asset family>

You cannot assign role <role name> to the search because the configuration cannot access the following field(s): <field name>, <field name>

Solution:

Use any of the following solutions to resolve this error:

1. Update the configuration and provide the role or user with access to the search.
2. Update the configuration and remove the hidden field from the search.
3. Do not allow the role to access the search.
4. Remove the configuration from the role.

Configuration Cannot Be Assigned to a Configured Search

Valid on all supported operating environments.

Symptom:

When attempting to provide a global or local configuration with access to a configured search, I receive an error similar to one of the following errors:

You cannot assign configuration <configuration name> to the search because the configuration cannot access the following field(s): <field name> on Asset Type <asset family>

You cannot assign configuration <configuration name> to the search because the configuration cannot access the Asset Type <asset family>

You cannot assign configuration <configuration name> to the search because the configuration cannot access the following field(s): <field name>, <field name>

Solution:

Use any of the following solutions to resolve this error:

1. Update the configuration and make the hidden field available to the search.
2. Update the configuration and remove the hidden field from the search.
3. Do not allow the configuration to access the search.

Chapter 3: Configuring the User Interface

This section contains the following topics:

Configurations

As an administrator, you can configure the user interface to simplify how users enter, manage, and search for data, protect users from performing unauthorized tasks, and help ensure that you conform to your IT asset management practices. When you configure the user interface, you, and all users affected by your configuration changes, immediately see the changes. For example, you do not want anyone, except the asset manager, to see any information for sites and companies. Therefore, you hide the Site and Company tabs and specify that only users in the asset manager role can see those tabs.

When configuring the user interface, use the following types of configurations:

- **Global configuration**. Configure the product for all users, regardless of their role.

  A *global configuration* lets you modify the functionality of your product implementation. You focus on configuring the pages, objects, fields, and so forth, for your specific implementation without having to make configuration changes for all possible users and roles.

  For example, you do not want to use the contact management functionality. In this situation, you define a global configuration on the Contact page, hide this functionality from all users, and save the global configuration. As a result, no users see the Contact page, unless you define a local configuration to override the global configuration.

  A global configuration can apply to all asset families or legal templates or to a specific family or template. You can have only one global configuration that applies to all families or templates or that applies to a specific family or template.

  Note: If you do not want to make any global user interface changes for your implementation, you do not have to define a global configuration. You can define a local configuration without defining a global configuration.

- **Local configuration**. Configure the product for specific users and roles.

  Use a *local configuration* to configure the user interface pages based on the requirements and needs of the different users and roles.

  Note: Local configuration changes override global configuration changes.

  For example, you define a global configuration to hide the contact management functionality in your implementation. However, there are users in a specific role who must be able to see and update contact information. In this situation, you define a local configuration on the Contact page, make the contact information appear, and save the local configuration. When you assign the local configuration to the users in the role, they see the contact information.

  A local configuration can apply to all asset families or legal templates or to a specific family or template. You can have multiple local configurations that apply to all families or templates or that apply to a specific family or template. You can assign to a role only one local configuration that applies to all families or templates or that applies to a specific family or template.

Important! You cannot assign a global configuration to a role. By default, a global configuration is assigned to all roles when the users log in and the security permissions for the roles are determined. You can only assign a local configuration to a role.

A global configuration is always assigned to all roles, even when you assign the role to a local configuration. Any permission from the global configuration that a local configuration does not override is applied to the role. Global configurations are used to configure the product for every user (except for the system administrator role, *uapmadmin*). To configure the user interface on a more detailed level by role, add a local configuration. In this situation, all users in all roles will see the configured interface based on the global configuration changes, and users assigned to a local configuration will see the additional changes to the interface.

If a user is assigned to a local configuration, the local configuration is assigned to the role when the user logs in.

Page Configuration by Asset Families and Legal Templates

For most objects, you configure the user interface, save the configuration, and all users in the role that is assigned to the selected configuration see the page that way. No additional configuration options are available. For certain objects (assets, models, and legal documents) you can provide a more specific configuration by selecting a particular *asset family* or *legal template, or all asset families or legal templates*.

You can manage pages in the following ways:

- Configure the model or asset page by asset family (see page 32).
- Configure the legal document page by legal template (see page 33).

Example: Configure for a Hardware and Software Asset

- (Hardware Asset) Configure the page for assets by moving important fields (asset name, model name, quantity, serial number, operating system, purchase order number, and service status) to the top of the page and making the fields required. In addition, remove the Host Name field. When you save the configuration, select the asset family *Hardware*. As a result, when users assigned to the configuration enter a hardware asset, they see the page as you have configured it.
- (Software Asset) Configure the page for assets by moving important fields (asset name, model name, quantity, serial number, department, cost center, and purchase order number) to the top of the page and making the fields required. In addition, remove the Service Status and Service Status Date fields. When you save the configuration, select the asset family *Software*. As a result, when users assigned to the configuration enter a software asset, they see the page as you have configured it.

Example: Configure Across All Asset Families

Configure the page for assets in all asset families by making the Requisition ID and Purchase Order ID fields read only for all users except the asset fulfiller. The asset fulfiller can edit these two fields. To achieve this result, you create two configurations:

1. A global configuration that makes the Requisition ID and Purchase Order ID fields read only. Select Across all families for this configuration so that the fields are read only on the Asset page for all asset families. This global configuration applies to all users.
2. A local configuration that allows users to edit the Requisition ID and Purchase Order ID fields. Select Across all families for this configuration, also, so that the fields can be edited on the Asset page for all asset families. This local configuration is assigned to users in the asset fulfiller role.

As a result, users who are not asset fulfillers cannot edit the Requisition ID and Purchase Order ID fields on the Asset page for any asset family. However, users in the asset fulfiller role can edit the two fields on the Asset page for all asset families.

Example: Configure for a Confidentiality Agreement

Configure the page for legal documents by moving important fields (Document Identifier, Effective Date, Termination Date, and Negotiator) to the top of the page and making the fields required. In addition, remove the Status and Status Date fields. When you save the configuration, select the legal template *Confidentiality Agreement*. As a result, when users assigned to the configuration enter a confidentiality agreement, they see the page as you have configured it.

Custom Asset Families

You can extend the product by creating additional asset families (see page 94) to track products other than hardware and software. *Custom asset families* let you track information about almost any classification of asset in your IT environment. For example, you can create asset families for telecommunications, services, and so on. After you create a custom asset family, configure the page and save the configuration for the custom asset family. As a result, a user assigned to the configuration for the custom asset family sees the page as you have configured it.

Configure the Model and Asset Page by Asset Family

You can configure the Model or Asset page for a specific asset family (for example, hardware asset and software asset) or for all asset families. Users in the role assigned to the configuration see the page as you have configured it.

Follow these steps:

1. Click the Model or Asset tab.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, select an asset family or select Across all families.

   Note: If you are creating a global configuration and a global configuration already exists across all families, the Across all families field does not appear.
4. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
5. Complete any of the following steps:
   - Change a field label (see page 46).
   - Move a field to a new location (see page 47).
   - Make a field read-only, required, or optional (see page 48).
   - Hide a field (see page 49).
   - Make a previously-hidden field appear (see page 50).
   - Add a field (see page 51).
6. Click Save Configuration.

   When you assign a configuration to a role (see page 21), users in the role see the page as you have configured it.

Configure the Legal Document Page by Legal Template

You can configure the Legal Document page for a specific legal template (for example, confidentiality agreement) or for all legal templates. Users in the role assigned to the configuration see the page as you have configured it.

Follow these steps:

1. Click the Legal Document page.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, select a legal template or select Across all templates.

   Note: If you are creating a global configuration and a global configuration already exists across all templates, the Across all templates field does not appear.
4. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
5. Complete any of the following steps:
   - Change a field label (see page 46).
   - Move a field to a new location (see page 47).
   - Make a field read-only, required, or optional (see page 48).
   - Hide a field (see page 49).
   - Make a previously-hidden field appear (see page 50).
   - Add a field (see page 51).
6. Click Save Configuration.

   When you assign a configuration to a role (see page 21), users in the role see the page as you have configured it.

How to Configure the User Interface

To configure the user interface, complete the following tasks:

- Protect users from performing unauthorized tasks using object access configuration (see page 35) and tab and menu configuration (see page 40).
- Make it easier for users to enter information for the objects they manage using field configuration (see page 46).
- Validate and enforce field format and data entry requirements using field data validation configuration (see page 58).
- Protect users from performing unauthorized tasks using hyperlink (see page 60) and button configuration (see page 61).
- Extend the repository to store more data using extended field configuration (see page 64).
- Extend the product and enhance how users enter information for the objects they manage using reference field configuration (see page 67).
- Extend the product and track more information and detail about an object using hierarchy configuration (see page 74).
- Make it easier for users to enter model, asset, and legal document information by family and legal template using page configuration (see page 30).
- Make it easier for users to find the objects they manage in searches using search configuration (see page 76).
- Make it easier for users to enter information for legal documents using legal template configuration (see page 89).
- Alert users about upcoming events and verify that the appropriate tasks are performed in the correct order at the right time using event and notification configuration (see page 91).
- Make it easier for users to select the correct items from lists using list management (see page 93).
- Extend the product and enhance how users manage object information using custom relationships (see page 96).

Object Access Configuration

You can configure object access to help protect the integrity of the data, prevent users from performing unauthorized tasks, and provide users with only the information appropriate for their job functions. You can configure object access in the following ways:

- Hide an object (see page 35). You do not want a user to be able to see pricing information for models. Therefore, you hide the Parts and Pricing area of the Models page.
- Make an object appear (see page 36). You want a user to be able to see pricing information for models. Therefore, you make the Parts and Pricing area of the Models page appear.
- Make an object read-only (see page 37). You want a user to be able to see, but not change, pricing information for models. Therefore, you make the Parts and Pricing area of the Models page read-only.
- Make an object accessible (see page 38). You want a user to be able to see, and edit, pricing information for models. Therefore, you make the Parts and Pricing area of the Models page accessible.
- Grant permissions to users to secure objects (see page 39).

Combine object access and field configuration to enforce more granular levels of access.

Hide an Object

You can hide an object to prevent users from seeing a particular area of the page for the object.

To hide an object

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. On the right, next to the title for the area of the page (for example, Models page, Parts and Pricing) click the Access Granted icon.

   The Access Denied icon appears for the object.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role cannot see the object information.

Make an Object Appear

You can make an object appear when users should be able to see a particular object.

To make an object appear

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. If access is already denied for the object, click the Access Denied icon on the right, next to the title for the area of the page (for example, Models page, Parts and Pricing).

   The Access Granted icon appears for the object.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see the object information.

Make an Object Read-Only

You can make an object read-only when users should be able to see, but not change the information about a particular object.

To make an object read-only

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. On the right, next to the title for the area of the page (for example, Models page, Parts and Pricing) click the Editable icon.

   The Read Only icon appears for the object.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see, but not change the object information.

Make an Object Accessible

You can make an object accessible when users should be able to see and change the information about a particular object.

To make an object accessible

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. If the object is already read-only, click the Read Only icon on the right, next to the title for the area of the page (for example, Models page, Parts and Pricing).

   The Editable icon appears for the object.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can access the object information.

Grant Permissions to Secure Objects

You can grant permissions to users so they can configure the user interface and hide objects, make objects appear, make objects read-only, and make objects accessible.

To grant permissions to secure objects

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON to enable the configuration of the page.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Secure (Read-Only And Access) to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to hide objects, make objects appear, make objects read-only, and make objects accessible.

Tab and Menu Configuration

You can configure tab and menu access to help protect the integrity of the data for your objects, prevent users from performing unauthorized tasks such as adding or deleting object information, and to support separation of duties so users only see the information appropriate for their particular job function.

Note: For assets, models, and legal documents, you provide a specific configuration by specifying the *asset family* (assets and models) and *legal template* (legal documents).

You can configure tab and menu access in the following ways:

- Hide a tab (see page 41). You do not want a user to be able to see any information for legal documents. Therefore, you hide the Legal Document tab.
- Make a tab appear (see page 41). You want a user to be able to see all information for legal documents. Therefore, you make the Legal Document tab appear.
- Make a tab read-only (see page 42). You want a user to be able to see, but not change, the information for a model. Therefore, you make the Model tab read-only.
- Make a tab accessible (see page 42). You want a user to be able to see, and edit, all information for a model. Therefore, you make the Model tab accessible.
- Hide a menu option (see page 43). You do not want a user to be able to view model dependencies. Therefore, you hide the Dependencies menu option.
- Make a menu option appear (see page 44). You want a user to be able to view model dependencies. Therefore, you make the Dependencies menu option appear.

- Make a menu option read-only (see page 44). You do not want a user to change any notes for a model. Therefore, you make the Notes menu option read-only.
- Make a menu option accessible (see page 45). You want a user to be able to change the generic configuration for a model. Therefore, you make the Model Configuration menu option accessible.

Combine tab and menu configuration and field configuration to enforce more granular levels of access.

Hide a Tab

You can hide a tab when users should not be able to see a particular tab.

To hide a tab

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. On the tab, click the Access Granted icon.

   The Access Denied icon appears for the tab.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role cannot see the tab.

Make a Tab Appear

You can make a tab appear when users should be able to see a particular tab.

To make a tab appear

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. If the tab is already hidden, click the Access Denied icon on the tab.

   The Access Granted icon appears for the tab.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see the tab.

Make a Tab Read-Only

You can make a tab read-only when users should be able to see, but not change the information on a particular tab.

To make a tab read-only

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. On the tab, click the Editable icon.

   The Read Only icon appears for the tab.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role cannot change the information on the tab.

Make a Tab Accessible

You can make a tab accessible when users should be able to view and change the information on a tab.

To make a tab accessible

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. If the tab is already read-only, click the Read Only icon on the tab.

   The Editable icon appears for the tab.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can access the information on the tab.

Hide a Menu Option

You can hide a menu option when users should not be able to see all, or a particular menu option.

To hide a menu option

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. On the menu or menu option, click the Access Granted icon.

   The Access Denied icon appears for the menu or menu option.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role cannot see the menu option.

Make a Menu Option Appear

You can make a menu option appear when users should be able to see all, or a particular menu option.

To make a menu option appear

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. If the menu or menu option is already hidden, click the Access Denied icon on the menu or menu option.

   The Access Granted icon appears for the menu or menu option.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see and use the menu option.

Make a Menu Option Read-Only

You can make a menu option read-only when users should be able to see, but not use a particular menu option.

To make a menu option read-only

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. On the menu or menu option, click the Editable icon.

   The Read Only icon appears for the menu option.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see, but not use, the menu option.

Make a Menu Option Accessible

You can make a menu option accessible when users should be able to see, and use a particular menu option.

To make a menu option accessible

1. Click the tab and optional subtab for the object access that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the object access is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration, or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. If the menu or menu option is already read-only, click the Read Only icon on the menu or menu option.

   The Editable icon appears for the menu option.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see, and use the menu option.

Field Configuration

You can change the display and attributes of field information on the page to meet your asset management practices and help make it easier for users to enter information for the objects they manage. In the product, these fields are referred to as *configured fields*.

You can manage fields in the following ways:

- Change a field label (see page 46).
- Move a field to a new location on the page (see page 47).
- Make a field read-only, required, or optional (see page 48).
- Hide a field (see page 49).
- Make a previously hidden field appear (see page 50).
- Add a field (see page 51).
- Grant permissions to change a field label (see page 52), move a field (see page 53), make a field required (see page 54), hide a field (see page 55), and perform mass changes (see page 56).
- View field information (see page 57).

Note: To make more extensive changes to a field, create an extended field (see page 64), which lets you define all attributes of a field.

Change a Field Label

You can change a field label to help make the field more familiar to users and conform to your IT asset management practices.

To change a field label

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. Click the field label and enter the new label.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role see the new field label.

Move a Field to a New Location

You can move a field to a new location to help make it easier for users to find the field on the page.

To move a field to a new location

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. Drag-and-drop the field to a new location in the current section.

   Note: You cannot move a field from one section of the page to another. For example, you cannot move a field from the Additional Information section to the Basic Information section.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role see the fields in the new location.

Make a Field Read-Only, Required, or Optional

A *required field* is a field that must contain a value to save the record. When you configure a field or create an extended field (see page 65), you can make the field read-only, required, or optional. Making a field required is useful for fields that contain key pieces of data.

Important! When making a new required field, saved records may not have data in the field. When you save the record in the future, you must enter data into the new required field. You must also enter data when a pre-existing record is updated by an application you write using the web services. Your client application must verify that the required field contains data, or provides data for the field. If not, the record will not be updated.

We recommend that before you make a field required, you populate the field for all existing records. You can search to locate all occurrences of blank values in the field by searching for NULL or space (clear the value field).

To make a field read-only, required, or optional

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. Next to the field, click the appropriate icon to make the field read-only, required, or optional.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role see the fields as read-only, required, or optional.

Hide a Field

You can hide a field from display when users should not be able to view a particular field on the page.

To hide a field from display

1. Click the tab and optional subtab for the object that you want to configure.

2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. Next to the field, click the Remove Field icon.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role do not see the field. If an event is defined for the hidden field, users still receive notifications. However, any mapped attribute that is not accessible in the workflow process associated with the event is not sent as part of the notification.

More information:

Event and Notification Configuration (see page 91)

Make a Previously-Hidden Field Appear

You can make a field appear when users must be able to see a field that you previous hid. For example, you previously hid the Capacity field. Users must be able to see that field because it is required. Add the field back so users can enter a value when defining an asset.

To make a field appear

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. Click Expose Hidden Fields.
5. Follow the on-screen instructions to add the field to the page.
6. Click Save Configuration.

   When you assign a configuration to a role, users in the role see the field on the page.

   Note: After you make a previously-hidden field appear, users can define an event for the field. You do not have to save the configuration because the field has already been added to the configuration. For more information about managing events, see the *User Guide*.

Add a Field

You can add a field to the page when users must be able to see a field that exists in the repository but is not part of a global configuration, or any field that has been removed and you have denied access. For example, you previously removed an extended field named chipset from the Asset Details page. Users must be able to see and enter a value for this field, so you add the field back onto the page. In addition, if you previously added an extension but did not save the global configuration, use these steps to add the extended field to the page.

Important! When you add a field to an object having multiple asset families (Assets and Models) and legal templates (Legal Documents), the field is added to all families and templates for the object, regardless of the family or template to which you added the field. For example, you add a field for the Hardware asset family. The field is added to all other asset families, including Computer, Other, Projects, Service, and Software.

To add a field

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration to the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global configuration (see page 29), or select an existing global configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! You can only add a field for a global configuration. You cannot add a field for a local configuration.

4. Click Save Configuration to create the global configuration.
5. Click Add Existing Fields.

   A wizard appears.
6. Select the fields to add to the page.

   Note: For extended fields, a link appears that matches the object label specified when defining an extended field (see page 65) (for example, asset hardware Extensions). Click the link and select the extended fields to add to the page.
7. Click Save Configuration.

   All users see the field on the page.

   Note: After you add a field and define an extended field, and save the field to a local or global configuration, users can define an event for the field. For more information about managing events, see the *User Guide*.

Grant Permissions to Change a Field Label

You can grant permissions to users so they can configure the user interface and change a field label.

To grant permissions to change a field label

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. In the Permissions area of the page, move Modify Labels to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to change a field label.

Grant Permissions to Move a Field

You can grant permissions to users so they can configure the user interface and move a field.

To grant permissions to move a field

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Order Fields to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to move a field.

Grant Permissions to Make a Field Required

You can grant permissions to users so they can configure the user interface and make a field required.

To grant permissions to make a field required

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Required to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to make a field required.

Grant Permissions to Hide a Field

You can grant permissions to users so they can configure the user interface and hide a field.

To grant permissions to hide a field

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Secure (Read-Only and Access) to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to hide a field.

Grant Permissions to Perform Mass Changes

You can grant permissions to users so they can configure the user interface and can perform mass changes on a field. You can perform mass changes on fields that are associated with the following objects:

- Asset
- Model
- Legal document
- Organization
- Contact
- Company
- Location
- Site

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Mass Change to the Granted Permissions list.

5. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to perform mass changes on a field.

View Field Information

You can view the information about any field, including extended fields, to see database-related field attributes. For any field, you can view the object label, database table name, database field name, attribute name, data type, description, and size. Use this information in the following ways:

- You want to view CA APM data outside of the product using an external reporting solution and must understand database-level information. For example, you want to know the database table name, field name, attribute name, data type, description, or field size for a particular default field or user-defined extended field.
- You have changed a field label (see page 46) or moved a field to a new location on the page (see page 47). Use the field information to understand how the field is represented in the database. This field information can be helpful when you work with Technical Support to understand any specific configuration changes you have made to the product.

To view field information

1. Click the tab and optional subtab for an object.
2. On the left, click CONFIGURE: ON.

   The configuration of the object is enabled.

3. Next to the field, click the View Details icon.

   The field information appears.

Field Data Validation Configuration

You can create field data validation configurations to validate the data entry in fields. These field data validations ensure that users enter data in the correct format and enforce your organizational business rules.

Note: The data validation affects new data that is added. Existing data records are not validated unless you access the data record and try to save the record.

For example, you want to ensure that users enter asset names using only alphanumeric characters (no special characters). Create a data validation for the Asset Name field on the New Asset or Asset Details page and specify that the field allows only alphanumeric entries. Users receive an error message if the characters they use are not alphanumeric.

You can create the following field data validation configuration:

Add a data validation for a text field (see page 58)

Add a Data Validation for a Text Field

You can validate the data entry in text fields (for example, contact name, email address, or telephone number) to enforce specific format requirements. You create the data validations for text fields by defining the regular expressions that apply to the different types of text fields.

Note: A *regular expression* is a text string that describes a particular pattern or format. Regular expressions are used to validate text to ensure that the text matches a predefined format. For example, create a regular expression to specify the correct format for an email address, telephone number, or IP address.

Important! Compose and test your regular expression before creating the text field data validation. You can find resources on the Web for creating, analyzing, and testing regular expressions.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 35), or select an existing configuration that you want to change.

      Note: Permissions for data validation are allowed by default. You can deny data validation permissions for the current configuration. The users assigned to the configuration do not then see the Data Validation icon and cannot add data validations.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles that are assigned to the selected configuration.

4. Next to the text field that you want to validate, click the Data Validation icon.

5. Enter the regular expression that applies to the type of field (for example, telephone number or email address) and click OK.

   Important! Verify that you selected the correct regular expression for the field type and that you entered the regular expression accurately.

   Note: To modify or delete an existing data validation, complete one of the following steps:

   - To modify the validation, edit the regular expression in the text entry field and click OK.
   - To delete the validation, clear the regular expression in the text entry field and click OK.

6. Click Save Configuration.

   When you assign the configuration to a role, users in the role receive data validation messages if their text entries do not match the defined format.

Hyperlink Configuration

You can configure hyperlink access to help prevent users from performing unauthorized tasks and only see the information appropriate for their particular job function. You can configure hyperlinks in the following ways:

- Hide a hyperlink (see page 60). You do not want a user to be able to see the audit history for an object. Therefore, you hide the View Audit History hyperlink.
- Make a previously-hidden hyperlink appear (see page 61). You hid the View Audit History hyperlink, but the hyperlink should now appear. Therefore, you make the View Audit History hyperlink appear.

Hide a Hyperlink

You can hide a hyperlink when users should not be able to see a particular hyperlink.

To hide a hyperlink from display

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. Next to the hyperlink, click the Access Granted icon.

   The Access Denied icon appears for the hyperlink.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role do not see the hyperlink.

Make a Previously-Hidden Hyperlink Appear

You can make a hyperlink appear when users must be able to see a hyperlink that you previous hid. For example, you previously hid the View Audit History hyperlink. Users must be able to see that hyperlink when defining assets, so you add the hyperlink back to the Asset page.

To make a hyperlink appear

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. If the hyperlink is already hidden, click the Access Denied icon next to the hyperlink.

   The Access Granted icon appears for the hyperlink.
5. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see and use the hyperlink.

Button Configuration

You can configure button access to help prevent users from performing unauthorized tasks. You can configure buttons in the following ways:

- Hide a button (see page 62). You do not want a user to be able to copy or delete an asset. Therefore, you hide the Copy and Delete buttons on the Asset page.
- Make a previously-hidden button appear (see page 63). You hid the Copy button for the Asset page, but the button should now appear. Therefore, you make the Copy button appear.

Hide a Button

You can hide options and buttons when you do not want users to be able to see and use the New menu option and the Save, Copy, and Delete buttons.

To hide a button from display

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:
   a. To hide the New option and Save button, move Create to the Denied Permissions list.
   b. To hide the Copy button, move Copy to the Denied Permissions list.
   c. To hide the Delete button, move Delete to the Denied Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role do not see the menu option and buttons.

Make a Previously-Hidden Button Appear

You can make buttons appear when users must be able to see and use the New menu option and the Save, Copy, and Delete buttons. For example, you previously hid the Copy and Delete buttons. Users must now be able to copy and delete objects, so you add the buttons back to the pages.

To make a previously-hidden button appear

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:
   a. To make the New option and Save button appear, move Create to the Granted Permissions list.
   b. To make the Copy button appear, move Copy to the Granted Permissions list.
   c. To make the Delete button appear, move Delete to the Granted Permissions list.
5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.
6. Click Save Configuration.

   When you assign a configuration to a role, users in the role can see and use the menu option and buttons.

Extended Field Configuration

You can design your own fields (*extended fields*) and add them to objects. Extended fields are additional fields to help ensure that you capture all data in your repository that is critical to the asset management program at your site. If you are not able to find an appropriate field in your repository to store key data, define an extended field for the data.

You can define extended fields for models, assets, legal documents, costs, payments, model parts and pricing, contacts, companies, organizations, locations, and sites. You can use extended fields when searching and for reports.

Note: You can add an extended field that you created for an asset cost to a legal document cost. Click Add Existing Fields on the Legal Document Cost configuration page.

Important! Extended fields are shared with the products integrating with CA APM (CA Service Desk Manager and CA Service Catalog). Therefore, any changes made to the extended field values in the integrating products are immediately reflected in CA APM. And, any changes you make to the extended field values in CA APM are reflected in the integrated products.

Define an Extended Field

You can define an extended field to help ensure that you capture all data in your repository that is critical to your asset management program. For example, when entering an asset for a blade server, there is no way to enter the chipset. Define an extended field named *chipset,* which adds the field to the Asset Details page. Users can enter the chipset information (for example, Intel 5520) with the other information such as the asset name, serial number, memory, processor, operating system, and so forth.

Important! These steps work only the first-time you complete the wizard and define the extended field for the object. Before you define the extended field, verify that you have the following information for reference: table name, label, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, field size, and whether an entry for the extended field is required. After you complete the wizard, you can configure the extended field like any field.

To define an extended field

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global configuration (see page 29), or select an existing global configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! You can only define an extended field for a global configuration. You cannot define an extended field for a local configuration.
4. Click Save Configuration to create the global configuration.
5. Click Add Extension.

   A wizard appears.

6. Select the Simple Field option and follow the on-screen instructions to enter the information for the extended field.

   Note: To change the default object label for the extended field, change the label in the Object Label field. For example, change the default label *asset hardware Extension* to *Hardware Extension*.

7. Click Save Configuration.

   All users see the extended field on the page.

   Note: After you add a field and define an extended field, and save the field to a local or global configuration, users can define an event for the field. For more information about managing events, see the *User Guide*.

Grant Permissions to Define an Extension

You can grant permissions to users so an Add Extension link appears to define an extension.

To grant permissions to define an extension

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global configuration (see page 29), or select an existing global configuration that you want to change.

   Important! You can only define an extended field for a global configuration. You cannot define an extended field for a local configuration.

4. In the Permissions area of the page, move Extend Object to the Granted Permissions list.
5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to define an extension.

Reference Field Configuration

You can define your own *reference fields* and add them to objects to extend the product and enhance how users enter information for the objects that they manage. When you define a reference field, you can reference an existing object, or define a new object.

- Define a reference field to an *existing object* to standardize on a common set of values that the user can select when defining an object. For example, when defining an asset, you want users to select the specific terms and conditions for an asset and select an approved general ledger code. In this example, you define two reference fields to standardize the terms and conditions and general ledger codes the user can select when defining the asset.
- Define a reference field to a *new object* to establish a relationship between people, companies, assets, and so forth. For example, when defining and managing vendors, you want the user to assign a service rating to each vendor and select a quality rating (one through five stars). In this example, you define one reference field to record the quality rating when defining and managing vendors.

You can define reference fields for models, assets, legal documents, costs, payments, model parts and pricing, contacts, companies, organizations, locations, and sites.

After you define a reference field, you can configure the field by completing the following tasks:

- Add a field to the reference field criteria and results (see page 70)
- Remove a field from the reference field lookup criteria and results (see page 71)
- Make a previously-hidden reference field appear (see page 72)
- Move a reference field to a new location (see page 73)

Define a Reference Field

You can define your own *reference fields* and add them to objects to extend the product and enhance how users enter information for the objects they manage. When you define a reference field, you can reference an existing object, or define a new object. For example, when defining an asset, you want users to select the specific terms and conditions for an asset and select an approved general ledger code. In this example, you define a reference field to an existing object and standardize the terms and conditions and general ledger codes the user can select when defining the asset.

Important! These steps work only the first-time you complete the wizard and define the reference field. Before you define the reference field, verify that you have the following information for reference: table name, label, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, field size, and whether an entry for the field is required. After you complete the wizard, you can configure the reference field by adding and removing fields, making a previously-hidden reference field appear, and moving a reference field to a new location.

To define a reference field

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global configuration (see page 29), or select an existing global configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! You can only define a reference field for a global configuration. You cannot define a reference field for a local configuration.
4. (Optional) Click Save Configuration to create the global configuration.
5. Click Add Extension.

   A wizard appears.
6. Select the Reference Field option and follow the on-screen instructions to enter the information for the reference field. The following fields require explanation:

   Object Label

   Displays the default reference field object label to appear when you add a field to the reference field criteria and results (see page 70), and make a previously-hidden reference field appear (see page 72). You can change this label to meet your requirements. For example, change the default label Location Extensions to Location.

   Label

   Enter the label for the reference field that you want to appear in list management.

   Service provider eligible

   Determines if field values from the service provider are included in the reference field. When you select this check box, public data and service provider objects are included in the reference field.

   Based on current object

   Select an existing object on which to base the reference field you are defining.

   Note: When you select this option, the reference field for the object already exists and the multi-tenancy options for the object are applied.

Object table name

Specify the database table name for the reference field.

Object Tenancy

If multi-tenancy is enabled, specify how multi-tenancy works for the reference field by selecting one of the following options:

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 will not see a tenant drop-down when entering data.

Note: When multi-tenancy is disabled, you do not see the Object Tenancy drop-down for the reference field. However, the product applies the Tenant Optional setting to the reference field. The product works this way so that if you enable multi-tenancy, the Tenant Optional setting is applied to the reference field.

7. Click Save Configuration.

All users see the reference field on the page. When you define a reference field based on a new object, the reference field appears as a list item that can be managed using list management (see page 93).

Add a Field

You can extend the information that appears in your reference field criteria and results by adding additional fields. For example, when users add an asset, they can search by model name and description to find the model describing the asset. You can configure the model reference field and add the Asset Family, Class, and Company Name fields to the reference field criteria and results to make it easier for users to find the model when defining the asset.

Note: When your assigned role has permissions to configure the object, you can complete this task.

To add a field to the reference field criteria and results

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. Click Save Configuration.
5. Next to the field, click the Lookup Field icon.

   A list of fields in the reference field criteria and results appears.
6. (Global configurations only) Click Add Fields.

   The Add Fields dialog appears.
7. Select the fields to add to the reference field criteria, results, or both.
8. Click Save.
9. Click Save Configuration.

   The field appears in the reference field criteria and results.

Remove a Field

You can remove a field when you do not want a particular field included in the reference field criteria and results. For example, you previously configured the model reference field by adding the Asset Family, Class, Company Name, and GL Code fields. To protect users from viewing sensitive information, you remove the GL Code field from the model reference field.

Note: When your assigned role has permissions to configure the object, you can complete this task.

To remove a field from the reference field criteria and results

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. Click Save Configuration.
5. Next to the field, click the Lookup Field icon.

   A list of fields in the reference field criteria and results appears.
6. Click the Mark for Deletion icon next to the field you want to remove from the reference field criteria and results.
7. Click Save.
8. Click Save Configuration.

   The field does not appear in the reference field criteria and results.

Make a Previously-Hidden Reference Field Appear

You can make a reference field appear when users must be able to see a reference field that you previously hid. For example, you previously configured the model reference field by removing the Inactive field. Add the field back to the model reference field so users can find and not select inactive models when adding an asset.

Note: When your assigned role has permissions to configure the object, you can complete this task.

To make a previously-hidden reference field appear

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. Click Save Configuration.
5. Next to the field, click the Lookup Field icon.

   A list of fields in the reference field criteria and results appears.
6. Click Expose Hidden Fields.

   The Expose Hidden Fields dialog appears.
7. Select the fields to add to the reference field criteria, results, or both.
8. Click Save.
9. Click Save Configuration.

   When you assign a configuration to a role, users in the role see the field in the reference field criteria and results.

Move a Reference Field

You can move a reference field to a new location to help make it easier for users to find the reference field. For example, you configure the model reference field and add the Asset Family, Class, and Company Name fields to the reference field criteria and results to make it easier for users to find the model when defining an asset. You move the Company Name field to the top of the model reference field so users can find models in a particular company.

Note: When your assigned role has permissions to configure the object, you can complete this task.

To move a reference field to a new location

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.
3. In the Configuration Information area of the page, complete the following steps:
   a. Specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.
   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.
4. Click Save Configuration.
5. Next to the field, click the Lookup Field icon.

   A list of fields in the reference field criteria and results appears.
6. Drag-and-drop the reference field to a new location in the reference field criteria and results.
7. Click Save.
8. Click Save Configuration.

   When you assign a configuration to a role, users in the role see the fields in the new location.

Hierarchy Configuration

In the product, a *hierarchy* is a way to establish a logical relationship to an object field. You can define a hierarchy to extend the product and track more information and detail about an object. You can define a hierarchy for any object.

Example: Create a Hierarchy to Locate an Asset

In CA APM, when you enter an asset, you can use the Location Name field to enter generic information related to the location of an asset (city and address). However, for a hardware asset family, you need a more detailed way to track the asset location. When you need to locate an asset for maintenance and repair, you must be able to find the specific office number, building number, floor number, and cubicle number. In this situation, define the following hierarchy:

```
Pittsburgh Office
    Building 3
        Fourth Floor
                Cubicle 49466
```

Note: In the previous hierarchy, each field is related to the field above it. If you change the information for a parent field (Building 3), the information for the child field (Fourth Floor and Cubicle 49466) is changed. However, changing a child field (Fourth Floor) does not change the parent field (Building 3).

By defining this hierarchy, you know and can track the exact location of the asset. In addition, CA APM manages the fields that you define in the hierarchy so they can be used in searches and reports.

Define a Hierarchy

You can define a hierarchy to extend the product and track more information and detail about an object. For example, define a location hierarchy for an asset to track the asset to a specific location. When a location is selected for the asset, and the location has a hierarchy established for the current asset family, a list appears inside the location section. Each location hierarchy extended field has one list. If the location selected has values for the hierarchy, the values are populated in the drop-down list.

Important! Before you define a hierarchy, verify that you have the following information for reference: table name, label, format (character, boolean, currency, date, decimal, or integer), field name, attribute name, field size, and whether an entry for the extended field in the hierarchy is required.

To define a hierarchy

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, complete the following steps:

   a. Specify the information for the new global configuration (see page 29), or select an existing global configuration that you want to change.

   b. (Optional) In the Object drop-down list, select the part of the object that you want to configure. Any permission changes you make (for example, deny permissions to move a field) apply only to that part of the object.

      For example, when configuring a legal document, you select Legaldoc Status History in the Object drop-down list. You deny permissions to move fields for that part of the object (the status history). The permission changes apply only to the status history part of the object, and not to the other parts of the object.

   Important! You can only define a hierarchy for a global configuration. You cannot define a hierarchy for a local configuration.

4. (Optional) Click Save Configuration to create the global configuration.

5. Click Add Extension.

   A wizard appears.

6. Select the Hierarchy option and follow the on-screen instructions to define the hierarchy. The following fields require explanation:

   Object Label

   Displays the default object label for the hierarchy. You can change this label to meet your requirements. For example, change the default label Asset Extensions to Asset.

   Object Table Name

   Specify the database table name for the hierarchy.

   Object Tenancy

   If multi-tenancy is enabled, specify how multi-tenancy works for the hierarchy by selecting one of the following options. The option you select is applied to all levels in the hierarchy.

   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. A tenant drop-down does not appear for users assigned to a role that only exposes a single tenant when entering data.

Begin with existing field

Select an existing field as the basis for fields in the first hierarchy level.

Begin with a new field

Select to start the hierarchy with a new field you define. You must define at least two levels for the hierarchy.

7. Click Save Configuration.

   All users see the hierarchy on the page.

Search Configuration

You can configure searches to simplify how users search for information in the repository and export the results. To configure searches, complete the following tasks:

- Set a search result limit (see page 77).
- Make it easier to search by assigning a default search for a role (see page 77).
- Make it easier to specify search criteria by completing the following tasks:
  - Adding fields (see page 79)
  - Removing fields (see page 79)
  - Moving fields (see page 80)
  - Changing the field name (see page 81)
  - Replacing fields (see page 82)
- Make it easier to find information in the search results by completing the following tasks:
  - Adding columns (see page 82)
  - Moving columns (see page 83)
  - Changing the column label (see page 84)
  - Removing columns (see page 84)
  - Adding sort fields (see page 85)
  - Preventing duplicate records from appearing (see page 85)

- Preventing the ability to open records (see page 86)

- Make it easier to search by allowing users to save searches (see page 86).
- Make it easier to use search results in spreadsheets by allowing users to export search results (see page 87).
- Delete a search that you do not need (see page 89).

Set a Search Result Limit

When you search for an object and the results are difficult to manage because too many object records appear, you can set a limit. For example, when you search for assets, over 2,000 assets appear in the search results. The results are difficult to navigate, you cannot find the assets you want, and the performance is negatively impacted. Therefore, you set a maximum of 50 object records to return.

To set a search result limit

1. Click the tab and optional subtab for the search that you want to configure.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. In the Additional Settings, Maximum Search Results Returning area, specify the total number of objects to appear.

   Note: For performance reasons, we recommend that you set this value to less than 500.
5. Click Go.

   The limited search results appear and help you see the impact on the results before you save the limit. All future search results are limited to the specified number or percentage.

Assign a Default Search for a Role

You can assign a default search for a role so that all users in the role have the same default search when they click a tab or subtab. For example, all users responsible for reviewing and negotiating contracts, agreements, and services belong to the Contract and Vendor Management role. To simplify the search setup for users so they do not have to specify a default search for themselves, you configure the default legal document search. You assign the configured legal document search as the default for all users in the Contract and Vendor Management role. When users in this role click the Legal Document tab, they see the configured legal document search as their default, rather than the default legal document search provided by the product.

Consider the following information when assigning a default search for a role:

- If you do not assign a default search for a role, the default search for the object appears when users in the role click the tab or subtab.
- You can assign multiple default searches for a role. However, you can only assign one default search for a particular object type (for example, model, asset, legal document, and so forth) to a role.
- When a user saves a search as their default, that search is the default for the user, even when you assign a different search as the default for the role. For example, a user in the Asset Technician role sets their default search as the asset search provided by the product. You configure the default asset search by adding a field to the search criteria and removing a field from the search results. You then assign the configured asset search as the default search for the Asset Technician role, to which the user belongs. The default asset search is the default for the user, even when you have assigned the configured asset search as the default for the role.
- A search must be available to a role before you can assign the search as the default for the role. For example, you create a legal document search. To make the search available to the Contract and Vendor Management role, assign the Contract and Vendor Management role to the search. You can then assign the legal document search as the default for the Contract and Vendor Management role.

  Note: For more information about assigning a role to a search, see Search Security (see page 25).

To assign a default search for a role

1. Click Administration, User/Role Management.
2. On the left, expand the Role Management menu.
3. Click Role Search.
4. Search for and select a role.

   The role details appear.
5. In the Default Searches area of the page, click Select New.
6. Select the default search for the role.

   The default search is added to the Default Searches list.
7. Click Save.

   The search is saved as the default for all users in the role.

Add a Field

CA APM lets you extend the information that appears in your search criteria and results by adding additional fields. For example, you can add the DNS Name field to the asset search. You can add fields to a new and saved search. You cannot add fields to the default searches provided by the product.

To add a field

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
5. Click Add Fields.

   The Add Fields dialog appears.
6. Select the fields to add to the search criteria, results, or both.
7. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
8. Click Save.

   The field appears in the search criteria and results.

Remove a Field

CA APM lets you remove a field when you do not want a particular field included in the search criteria. For example, you can remove the DNS Name field from the asset search.

To remove a field from the search criteria

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches appears.

3. Click a search in the list.
4. Complete the following steps:
   a. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   b. Click the appropriate icon next to the field in the search criteria.
   c. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
5. (Optional). Complete the following steps:
   a. In the search criteria area of the page, click Advanced.
   b. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   c. Click the Mark for Deletion icon next to the field you want to remove from the search criteria.
   d. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
6. Click Save.

   The field is removed from the page and does not appear in the search criteria.

Move a Field

CA APM lets you move a field in the search criteria to a new location to help make it easier for you to enter your search criteria. For example, you can move the Bar Code Number field so that the field appears before the Serial Number field.

To move a field to a new location

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
5. Drag-and-drop the field to a new location in the search criteria.
6. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.

7. Click Save.

   The new location of the field is saved.

Change the Field Name

CA APM lets you change the label for a field to help make the field name more familiar in your search criteria. For example, you can change the label *Asset Quantity* to *Quantity*.

To change the field name

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches appears.
3. Click a search in the list.
4. Complete the following steps:

   a. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   b. In the search criteria, click the field label and enter the new label.

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

   The configuration of the search is complete.
5. (Optional). Complete the following steps:

   a. In the search criteria area of the page, click Advanced.

   b. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

   c. Click the Edit Record icon next to the field for which you want to change the label.

   d. Enter the new field label.

   e. Click the Complete Record Edit icon.

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

   The configuration of the search is complete.
6. Click Save.

   The new field label appears in the search criteria.

Replace a Field

CA APM lets you replace an existing field in your *advanced* search criteria with a different field. For example, when searching for companies, you can replace the field *Company ID* with *Company Name*.

Note: You can replace fields only in a custom search that you created. You cannot replace fields in the product default search.

To replace a field

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches appears.
3. Click a search in the list.
4. Complete the following steps:
   a. In the search criteria area of the page, click Advanced.
   b. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
   c. Click the Search icon next to the field that you want to replace with a different field.

      The Add Fields dialog appears.
   d. Select the replacement field and click OK.
   e. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
5. Click Save.

   The existing field is replaced in the search criteria.

Add a Column

CA APM lets you add a new column to the search results to help make it easier for you to find the information you need in search result lists. For example, you have several people in your enterprise with the name John Smith. Their first and last names are the same, but their additional contact information (email address, supervisor, department, and so forth) is different.

When you search for a contact and specify *John* as the first name and *Smith* as the last name, two instances of John Smith appear in the search results. Add an email column to the results so that two unique instances of John Smith appear:

- John Smith (John.Smith1@company.com)
- John Smith (John.Smith2@company.com)

You can add columns to a new and saved search. You cannot add columns to the default searches provided by the product.

To add a column to the search results

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
5. Click Add Fields.

   The Add Fields dialog appears.
6. Select the fields to add to the search results.
7. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
8. Click Save.

   The column is added to the search results.

Move a Column

CA APM lets you move a column to a new location to help make it easier for you to find the information you need in the search results. For example, you can move the Asset ID column so that the column appears before the Asset Name column.

To move a column to a new location

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.

5. In the search results list, drag-and-drop the column to a new location.
6. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
7. Click Save.

   The new location of the column is saved.

Change the Column Label

CA APM lets you change the label for a column heading to help make the label more familiar in your search results. For example, you can change the label *Asset Quantity* to *Quantity*.

To change a column heading label

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
5. In the search results, select the column heading and enter the new label.
6. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
7. Click Save.

   The new column label appears in the search results.

Remove a Column

CA APM lets you remove a column when you do not want a particular column included in the search results. For example, you can remove the Mac Address column from the search results.

To remove a column

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.

3. Click a search in the list.
4. At the top of the page, click CONFIGURE SEARCH: ON.

   The configuration of the search is enabled.
5. In the search results, click the appropriate icon next to the column.
6. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
7. Click Save.

   The column is removed from the page and the search results.

Add a Sorting Field

CA APM lets you add sorting fields to the search results and extend the default sort of a single column using either ascending or descending order. For example, you currently sort assets by asset name. You can add asset family to the sorting so that you can sort on both asset name and asset family.

To add a field to sort the search results

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. In the Additional Settings, Search Result Sorting area, add the additional field for sorting.
5. Click Go.

   The results appear with the extended sorting and help you see the impact on the results before you save the sorting. The new field is added and you can use the field to sort the search results.

Prevent Duplicate Object Records

CA APM lets you prevent duplicate object records from appearing in the search results. For example, you have several people in your enterprise with the name John Smith. Their first and last names are the same, but their additional contact information (email address, supervisor, department, and so forth) is different.

You have a saved contact search in which only the first and last name of the contact appears in the results. When you search using the saved contact search and specify *John* as the first name and *Smith* as the last name, two instances of John Smith appear in the search results. When you prevent duplicate records from appearing, only one instance of John Smith appears.

To prevent duplicate object records from appearing in the search results

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click the search for which you want to prevent duplicate records from appearing.
4. In the Additional Settings, Unique Search Characteristics area, select the Make Results Unique check box.
5. Click Go.

   The results appear without the duplicate records and help you see the impact on the results before you save your settings. The DISTINCT argument is added to the SQL statement, preventing duplicate records from appearing in the search results.

Prevent Opening Records

CA APM lets you disable the ability to open individual records from the search results. For example, you do not want users to open and display contact information from the contact search results.

To prevent opening object records from the search results

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.
3. Click a search in the list.
4. In the Additional Settings, Unique Search Characteristics area, clear the Allow Selection of Results check box.
5. Click Save.

   A hyperlink does not appear in the search results to open the object.

Allow Users to Save Searches

You can grant permissions to users so a Save button appears to save searches.

To allow users to save searches

1. Click the tab and optional subtab for the object you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:

   Note: When you grant any combination of the following permissions, the user can save searches.

   a. To allow only the current user who is logged in to save a search, move Save Search to User to the Granted Permissions list.

   b. To allow the current user who is logged in and specific configurations to save a search, move Save Search to Configuration to the Granted Permissions list. The search is available to the current user and all users that you select for the configuration.

   c. To allow the current user who is logged in and specific roles to save a search, move Save Search to Role to the Granted Permissions list. The search is available to the current user and all users in the roles you select.

5. Click Save Configuration.

   The configuration is saved. Verify that you correctly assign a configuration to a role.

Allow Users to Export Search Results

You can grant permissions to users so they can save exported search results.

To grant permissions to export search results

1. Click the tab and optional subtab for the object you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, specify the information for the new global or local configuration (see page 29), or select an existing configuration that you want to change.

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, complete the following steps in the Granted and Denied Permissions lists:

   Note: When you grant any combination of the following permissions, the user can save exported search results.

   a. To allow only the current user who is logged in to save the exported search results, move Export for User to the Granted Permissions list.

      Note: When this is the only permission granted to a user, the user cannot select the Export to All Configurations assigned on Search and Export to All Roles assigned on Search check boxes when scheduling search requests. For information about scheduling search requests, see the *User Guide*. An email is sent to the current user only. The email includes a link to the CSV file or specifies the name of the database view, depending on the type of export.

   b. To allow the current user who is logged in and specific configurations to save the exported search results, move Export for Configuration to the Granted Permissions list. The export is available to the current user and all users in the selected configurations assigned to the search used by the export.

      Note: When this permission is granted to a user, the user can select the Export to All Configurations assigned on Search check box when scheduling search requests. For information about scheduling search requests, see the *User Guide*. An email is sent to all users in the selected configurations. The email includes a link to the CSV file or specifies the name of the database view, depending on the type of export.

   c. To allow the current user who is logged in and specific roles to save the exported search results, move Export for Role to the Granted Permissions list. The export is available to the current user and all users in the selected roles assigned to the search used by the export.

      Note: When this permission is granted to a user, the user can select the Export to All Roles assigned on Search check box when scheduling search requests. For information about scheduling search requests, see the *User Guide*. An email is sent to all users in the selected roles. The email includes a link to the CSV file or specifies the name of the database view, depending on the type of export.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   The configuration is saved. Verify that you can correctly assign a configuration to a role.

Delete a Search

You can delete a saved search (default and user-defined search) that you do not need.

To delete a saved search

1. Click the tab and optional subtab for the object that you want to find.
2. On the left, click Manage Searches.

   A list of saved searches displays.

3. Click the search that you want to delete.
4. Click Delete and confirm that you want to delete the search.

   The search is deleted.

Legal Template Configuration

A *legal template* provides the group of attributes that belong to a particular type of legal document. You typically set up and maintain legal templates, while users create legal document records based on the legal templates. When you create a legal document record, you first select a legal template on which to base the document. The legal document record inherits the attributes from the legal template.

Each legal template has *terms and conditions* that typically apply to the legal document type. For example, a legal template for an invoice may include information about the terms of payment.

You can use the product to define legal templates and change the attributes of a legal template. If you want to change the terms and conditions assigned to a legal template, you can remove them or add new ones from the master list of terms and conditions.

A legal template cannot be deleted until all legal documents based on the template are deleted. In addition, you can search for legal documents by the legal template name, and you can use legal template names to select records to include in reports.

Define a Legal Template

You can define a legal template to group attributes that belong to a particular type of legal document. Administrators or users with appropriate privileges can define legal templates.

To define a legal template

1. Click Directory, List Management.
2. On the left, expand Legal Document Lists and click Legal Template.

   The list of templates appears on the right.
3. Click New, enter a name for the template, and click Save.

   The new template appears in the list.
4. Click the Edit Record icon for the new template.
5. Click the View Assigned Ts & Cs hyperlink.
6. Click Select New and select the terms and conditions for the new template.
7. Click Save.

   Users can select the new template when they define legal documents.

Change the Terms and Conditions for a Legal Template

You can change the terms and conditions for a legal template. Administrators or users with appropriate privileges can change the terms and conditions.

To change the terms and conditions for a legal template

1. Click Directory, List Management.
2. On the left, expand Legal Document Lists and click Legal Template.

   The list of templates appears on the right.

3. Click the Edit Record icon for the legal template.
4. Click the View Assigned Ts & Cs hyperlink.

   All terms and conditions for the legal template appear.
5. Select any of the following options:
   - Click Select New and select the terms and conditions for the template.
   - Click the Delete icon to remove the term and condition from the template.
6. Click Save.

   The updated terms and conditions are applied to the template.

Event and Notification Configuration

An *event* represents an activity related to a field (default or extended) for an object. When you define an event, you specify the criteria that must be met before the event occurs. For example, you want to know when the data in a particular field changes. You can define an event that detects the data change. An event works in combination with a *notification*, which the workflow provider (for example, CA Process Automation) creates to alert your team members that an important event has occurred for a specific field or object. By using events and notifications, you alert people about upcoming events and help ensure that the appropriate tasks are performed in the correct order at the right time.

A notification is triggered when an event that you define occurs. For example, you define a date event on the Termination Date field for a legal document to notify the contract manager 15 days before a legal contract expires. The contract manager uses the 15 days to review and possibly negotiate a better contract. When the date arrives (that is, 15 days before the contract expires), the event occurs and the notification process is triggered through the workflow provider. The workflow provider constructs, issues, and manages the notification based on the configuration that you provided in the workflow provider and in CA APM.

The default notification method in CA APM supports email notifications using a workflow provider. You can send an email notification to any user or distribution list that is defined in your internal email system, even if the user is not a CA APM user. In addition, you can send an email to any external email address, if permitted by your email system.

You can also configure the notification process in the workflow provider to trigger any type of process. For example, you can set up the notification process to perform certain actions in another application when an event occurs in CA APM. For information about setting up different notification processes, see your workflow provider documentation.

You can define the following types of events to track and manage important changes to fields or objects:

- Date events. Monitor a date field for an object and have the workflow provider notify you that an important date is approaching or has passed.
- Change events. Monitor a field for an object and have the workflow provider notify you that the field value has changed.
- Watch events. Monitor a field for an object and have the workflow provider notify you about a potential obstruction to completing a task.

How to Configure Events and Notifications

Events work in combination with notifications, which the workflow provider (for example, CA Process Automation) creates, to communicate information to your team members about important events and activity. To configure events and notifications, complete the following steps:

1. Administrators grant permissions to users to manage events (see page 92).
2. Users with the correct permissions open an existing configuration and define date events, change events, and watch events.

   Note: For more information about defining events, see the *User Guide*.
3. Users, when defining an event, map all workflow provider process parameters to a CA APM object attribute.

   Note: For more information about mapping workflow provider process parameters, see the *User Guide*.
4. The workflow provider initiates the notification process.
5. Users view an audit history of events.

   Note: For more information about viewing an audit history of events, see the *User Guide*.

Grant Permissions to Manage Events

You can grant permissions to users so they can configure the user interface and define an event.

To grant permissions to define an event

1. Click the tab and optional subtab for the object that you want to configure.
2. On the left, click CONFIGURE: ON.

   The configuration of the page is enabled.

3. In the Configuration Information area of the page, select an existing global or local configuration (see page 29).

   Important! Global configuration changes affect all users, regardless of their role. Local configuration changes only affect users in the roles assigned to the selected configuration.

4. In the Permissions area of the page, move Manage Events to the Granted Permissions list.

5. (Optional) Select the Inherit Permissions from Parent Object check box to apply any security permissions from a top-level (parent) object to the lower-level (child) object using the same configuration.

   For example, you create a local configuration for an Organization. In the configuration, you deny permissions to change field labels, move fields, make fields required, and hide fields. After you save the configuration, you open Attachments under Organization and select the Inherit Permissions from Parent Object check box. All permissions from the Organization are applied to Attachments. In this example, because permissions to change field labels, move fields, make fields required, and hide fields are applied to the Organization, the permissions are also applied to the Attachment.

6. Click Save Configuration.

   When you assign a configuration to a role, users in the role have permissions to define an event.

List Management

You can define the items that appear in lists to help make it easier for users to select the correct information from lists for the objects they manage. For example, when defining a new contact, the user can specify a contact type. You define the items that appear in the contact type list. In addition, when defining a legal document, the user must specify a legal template. You define the items that appear in the legal template list.

You can manage items in the following lists and in the reference fields you define:

- Assets
- Companies
- Contacts
- Legal Documents
- Locations
- Models

- Organizations
- Searches
- Normalization

Manage List Items

You can define, update, and delete list items to help make it easier for users to select the correct information from lists when managing objects. For example, you can change the name and description of a cost center to make it easier for users to select a cost center. You can also delete a general ledger code so that users cannot select that code when they define assets.

Important! When you delete a list item, users cannot select the item when defining an object. Instead of deleting the list item, you can make the list item inactive. Then, if you need the list item in the future, you can make the item active again. You do not have to redefine the item.

Follow these steps:

1. Click Directory, List Management.
2. On the left, select the list that you want to manage.
3. **Define a list.**
   a. Click New.
   b. Enter the information for the list item.

      Note: When multi-tenancy is enabled, select the tenant for the list item.
4. **Update a list.**
   a. Click the Edit Record icon next to the list item you want to update.
   b. Enter the new information for the list item.

      Note: To make a list item inactive, select the Inactive check box.
5. **Delete a list item.** Click the Mark for Deletion icon next to the list item you want to delete.
6. Click Save.

Define the Class and Subclass Lists for an Asset Family

You can define the class and subclass lists for an asset family to help make it easier for users to select the correct information when defining models and assets. For example, you can define the class "printer" and the subclass "laser". Then when users create or search for printer assets, this additional information helps them to define or identify the correct assets.

Follow these steps:

1. Click Directory, List Management.
2. On the left, click Asset Lists, Asset Family.
3. Complete the following steps to define the class list:
   a. Click the Edit Record icon next to the asset family for which you want to define the class.
   b. Click the Class List hyperlink.
   c. Define the class record for the asset family.
   d. Click Save.
4. Complete the following steps to define the subclass list:
   a. Click the Edit Record icon next to the class record for which you want to define the subclass.
   b. Click the Subclass List hyperlink.
   c. Define the subclass record for the asset family.
   d. Click Save.

Define Legal Document Terms and Conditions

You can define the terms and conditions that apply to legal document lists. Users can then apply the correct terms and conditions when they define legal templates or legal documents.

Follow these steps:

1. Click Directory, List Management.
2. On the left, expand Legal Document Lists and select Terms and Conditions.
3. Click New.
4. Enter the information for the new list item.

   Note: Select the Date Specific Key check box to make the new item apply to date-specific terms and conditions lists only. Clear this check box to make the new item apply to non-date-specific terms and conditions lists only.
5. Click Save.

Exclude an Asset Family

You can exclude an asset family so that it is not available for users. If you exclude an asset family, a user who creates or modifies a model cannot select that asset family. Also, the excluded asset family is not available for managing filters, data imports, or configurations. For example, if CA APM is integrated with CA Service Desk Manager, the asset families from CA Service Desk Manager are also available to CA APM users. If you do not require the CA Service Desk Manager asset families, you can exclude them so that they are not available to users.

If a model was already associated with an asset family before you excluded the family, you can still access and edit that model. You can also still use that model to create assets. However, you cannot change the asset family for that model to another excluded asset family.

Note: You can change the asset family for a model only if the model does not have associated assets.

Follow these steps:

1. Click Directory, List Management.
2. On the left, select Asset Family under Asset Lists or Model Lists.
3. Click the Edit Record icon for the family that you want to exclude.
4. Clear the Is ITAM check box and click the Complete Record Edit icon.

   Important! Do not select the Inactive check box. This action makes the asset family inactive for all products that are integrated with the CA MDB.
5. Click Save.

Custom Relationships

Custom relationships are links between two related objects. The relationship describes and provides information about the interdependencies between the objects. Through a custom relationship, you can navigate from one object to the other object. You can locate, retrieve, and modify information about the objects.

Manage Custom Relationships

You can define and update custom relationships between two objects. In a custom relationship, one of the objects is a primary object and the other object is a secondary object.

Note: You cannot delete a custom relationship that you define and save.

Follow these steps:

1. Define a custom relationship.
    a. Click the tab and optional subtab for the object for which you want to define a custom relationship.
    b. Select CONFIGURE: ON from the search results page.
    c. Select a global configuration across all families or templates or create and save a global configuration.

       Note: You cannot define a custom relationship for a local configuration.
    d. Click Add Custom Relationship.

       The Add Custom Relationship dialog opens.
    e. Specify a name for the primary object relationship and secondary object relationship.
    f. Select the secondary object.

       Note: For assets, models, and legal documents, select a family or template or select across all types.
    g. Click Save.

       The new custom relationships are displayed under the Custom Relationship menu for the primary and secondary objects.
    h. (Optional) Add simple or reference extended fields to the custom relationship.
2. Update a custom relationship.
    a. Click the tab and optional subtab for the object for which you want to update a custom relationship.
    b. Select CONFIGURE: ON from the search results page.
    c. Select a global configuration across all families or templates.
    d. Select the relationship under the Custom Relationship menu.
    e. Modify the information for the custom relationship and click Save.

Chapter 4: Managing Hardware Assets

This section contains the following topics:

Hardware Reconciliation

The hardware reconciliation process matches *discovered assets* to corresponding *owned assets* from different logical repositories so that you can manage the assets based on your business practices. Use this process to identify the discrepancies between your owned and discovered assets. Hardware reconciliation identifies unauthorized, missing, under-utilized, and over-utilized assets, which helps you to optimize your hardware asset base.

- Owned assets provide IT asset information from a financial and ownership perspective. The product supports the entire lifecycle of an owned asset from procurement, acquisition, allocation, use, and disposal, including legal and cost information. Owned assets have purchase records, including a purchase order number, invoice number, associated costs (lease, payment schedule, maintenance), associated contracts (terms and conditions), and vendor information. The owned-asset data is entered and imported using the CA APM user interface, Administration tab, Data Importer.
- Discovered assets provide information about the assets that an enterprise is using or has deployed. External discovery products and the discovery component of CA Client Automation scan the assets on a network and store them as discovered assets in the CA MDB. Discovered assets contain evidence about the following information:
  - The asset is deployed and can be found on your network.
  - The asset is being used and has metrics.
  - The asset contains up-to-date configuration information for inventory.

The CA APM hardware reconciliation process matches the discovered asset data and the owned asset data that are stored in the CA MDB. The hardware reconciliation process may detect assets that cannot be reconciled with any of your owned assets. You can decide to add the unreconciled assets to your repository so that you can track and manage all assets in your network.

Hardware reconciliation automates the synchronization of ownership and discovered data. Hardware reconciliation supports the discovery component of CA Client Automation and third-party discovery products. These components and products are supported through the combination of the CA Asset Converter and the asset collector component of CA Client Automation. When CA SAM is installed, discovery connectors load the discovery data into the CA SAM repository. The discovery data is then synchronized with CA APM.

Hardware Reconciliation Engine

The *Hardware Reconciliation Engine* is a continuously processing Windows service that is responsible for the following tasks during the reconciliation process:

- Synchronizes discovered assets with ownership assets using reconciliation rules (see page 113).
- Reconciles owned and discovered assets based on asset matching criteria (see page 115).
- Maps discovery data to ownership data based on normalization rules (see page 101).
- Updates selected asset fields in the product based on changes to the corresponding discovered assets.
- Completes the actions that are defined in the reconciliation rule that is being executed.

How Reconciliation Engines Process Reconciliation Rules

The date and time at which a reconciliation rule was last executed determines when the rule will be processed again. Hardware Reconciliation Engines process reconciliation rules in the following sequence, which allows for multiple tenant support as well as multiple Hardware Engines:

1. Each Hardware Reconciliation Engine searches for reconciliation rules that are not being processed by another engine and selects the rule that has the oldest processing date and time.
2. A Hardware Reconciliation Engine locks the reconciliation rule so it cannot be accessed by another engine, executes the rule, updates the rule date-and-time value, and then unlocks the rule. The Hardware Reconciliation Engine searches for the next available reconciliation rule with the oldest date-and-time value and repeats the process.
3. The process continues with all engines continuously operating and searching for and executing the next available reconciliation rule with the oldest date-and-time value.

How to Reconcile

The reconciliation process compares data from discovery products with CA APM ownership data in the CA MDB. This process reconciles discovered and owned assets, tracks changes to critical fields, and tracks discrepancies as the result of missing or deleted assets. To reconcile, complete the following steps:

1. Establish data normalization rules (see page 101) to map data values between discovery repositories and the product.
2. Define a reconciliation rule (see page 113) to specify how to limit the data being processed and how to process the records found.
3. (Optional) Define reconciliation update options (see page 114) 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 (see page 115) to match owned and discovered assets for a reconciliation rule.
5. (Optional) Exclude an ownership asset from the reconciliation process (see page 118).
6. (Optional) Exclude an asset family from the reconciliation process. (see page 119)
7. View the reconciliation results in the message queue (see page 121).
8. (Optional) Add unreconciled assets (see page 122) to your repository so that you can track and manage all assets in your network.

   Note: You can generate reports to view information about your reconciliation results and environment. For more information about generating reports, see the *User Guide*.

Data Normalization

Data normalization is a step in the reconciliation process where you establish a list of rules to standardize, organize, and consolidate data between the product and discovery repositories. Normalization reduces, eliminates, and consolidates redundant data that is imported into the product from multiple sources, such as purchase order products, human resource products, procurement products, the Data Importer, and so forth.

When you normalize data, you reduce the time and effort necessary to manage the data. You also reduce the possibility of the user selecting the incorrect information when defining assets, models, and other objects, and when generating reports. The product guides you through the normalization process, enabling you to perform it much more efficiently and accurately. The consolidated discovery data is then reconciled with your owned assets during the reconciliation process and can be reported on using the reconciliation reports.

You normalize three of the fields that can be used as asset matching criteria (see page 115): company, operating system, and system model. These fields are normalized because they often have multiple values that represent one normalized value. For example, the discovery tool may find many variations for the name of one company. You normalize all the variations to one value for the company name and include the normalized company name in asset matching criteria. These fields are normalized so that you can include them in asset matching criteria.

The Hardware Reconciliation Engine normalizes the data that is imported into the product by referencing the following normalization rules, which you define:

- Company normalization rules (see page 103)
- Operating System normalization rules (see page 106)
- System Model normalization rules (see page 109)

Example: Normalize Company Data

In this example, when you import company data into the product using CA Client Automation, multiple variations of Document Management Company are discovered in various formats, including the following values:

- Document Management Company
- Document Management Co
- Doc Management Company
- Doc Management Co

To help users select the correct company when defining an asset and model and when generating reconciliation reports, you define company normalization rules to map all variations to Document Management Company. During the reconciliation process, the normalization rules map the values as follows, before an asset is updated in the CA MDB:

Note: A collected company that is mapped to an authoritative company affects Hardware Reconciliation only if the collected company is a discovered company.

Collected (Nonauthoritative Value)	Normalized (Authoritative Value)
Document Management Co	Document Management Company
Doc Management Company	Document Management Company
Doc Management Co	Document Management Company

Company Normalization Rules

Company normalization rules are intended for key organizations with which you have a business relationship, for example, Microsoft, Adobe, Lenovo, and so forth.

Collected Company

A *collected company* is either a discovered company or a *product-defined company*. Product-defined companies are collected from user input and other products that share the CA MDB. Hardware reconciliation reconciles only *discovered* companies. Collected companies have a *nonauthoritative* status. You map nonauthoritative collected companies to normalized *authoritative* companies.

Important! Only *discovered* collected companies that are mapped to normalized companies are reconciled during Hardware Reconciliation.

Normalized Company

A normalized company is either a *CA-content company* or a product-defined company. CA-content companies are provided with CA APM and have an *authoritative status*. Authoritative status allows a company to have a normalization rule. You define a normalization rule for an authoritative normalized company when you map one or more collected companies to the authoritative company.

Product-defined companies initially have a nonauthoritative status. You can change the status of a product-defined company (see page 105) from nonauthoritative to authoritative. You can then map a collected company to the authoritative product-defined company to define a normalization rule. Only company normalization rules for discovered collected companies affect Hardware Reconciliation.

Subordinate Company

When you map a collected nonauthoritative company to a normalized authoritative company, the nonauthoritative company becomes *subordinate* to the authoritative company in the normalization rule.

Define Company Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can define company normalization rules that are applied during the matching process whenever the reconciliation rule contains asset matching criteria (see page 115). Any asset matching criterion that contains company information automatically applies the company normalization rules.

When you map a collected nonauthoritative company to a normalized authoritative company, the nonauthoritative company becomes *subordinate* to the authoritative company in the normalization rule. The subordinate company no longer appears in the Collected Company list or the Normalized Company list. If you delete the normalization rule (see page 111) that contains the subordinate company, the subordinate company returns to nonauthoritative status and appears in the Collected Company list and, if it was a product-defined company, also in the Normalized Company list.

To define company normalization rules

1. Click Directory, List Management.
2. On the left, expand Normalization and select Company Normalization.

   The discovered collected company values and the normalized company values appear.
3. If the term you want to use as the normalized value does not appear in the Normalized Company list or the Collected Company list, click New Company to add the company, and then repeat the previous steps.
4. (Optional) Change a nonauthoritative company to an authoritative normalized company (see page 105).
5. Map the Collected Company list discovered values to a Normalized Company value.

   The list of company normalization rules is defined and is referenced during the reconciliation process.

More information:

Company Normalization Rules (see page 103)

Update Company Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You update a company normalization rule when you want to change how a discovered company is normalized. This update may affect the reconciliation process. To update a normalization rule for a company, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change a normalization rule, the Hardware Reconciliation Engine processes the asset matching so that the assets are matched using the new rule. Any assets that are matched as a result of a previous Hardware Reconciliation Engine process are evaluated again to determine if their matching should change based on the new normalization rule.

When you delete a company normalization rule, the subordinate company returns to nonauthoritative status and appears in the Collected Company list. If the subordinate company was a product-defined company, it also appears in the Normalized Company list on the Normalization Rule page.

To update company normalization rules

1. Click Directory, List Management, Company Rules.
2. Delete the normalization rule (see page 111) that you want to change.
3. Define the new company normalization rule (see page 104).

More information:

Company Normalization Rules (see page 103)

Change a Nonauthoritative Company to an Authoritative Normalized Company

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can map collected companies to only authoritative companies in the Normalized Company list on the Company Normalization page. Product-defined companies in the Normalized Company list initially have a nonauthoritative status. You can change a product-defined company that is in the Normalized Company list to an authoritative normalized company, to which you can map collected companies.

Note: Only company normalization rules for discovered collected companies affect Hardware Reconciliation.

To change a nonauthoritative company to an authoritative normalized company

1. Click Directory, List Management.
2. On the left, expand Normalization and select the normalization type.

   The discovered collected values and the normalized values appear.
3. Clear the Show only Authoritative records check box in the Normalized Company section.
4. Click Go in the Normalized Company section.

   The collected product-defined companies that are nonauthoritative and not yet mapped to an authoritative company appear in the normalized list with an Override icon next to the company name.
5. Click the Override icon to the left of the nonauthoritative company that you want to change to an authoritative company, in the *normalized* list.

   The nonauthoritative company changes to an authoritative normalized company.
6. Map a collected company to the new authoritative normalized company before performing any other action in the Normalized Company section.

   Note: The company is not saved as an authoritative company until at least one collected company is mapped to the new authoritative company.

   The new authoritative normalized company and its normalization rule are saved.

More information:

Define Company Normalization Rules (see page 104)
Company Normalization Rules (see page 103)

Operating System Normalization Rules

Operating system normalization rules are intended for operating systems managing your computers, for example, Windows XP Professional, Windows Server 2008 Enterprise Edition, Windows Vista Enterprise Edition, and so forth.

Collected Operating System

A collected operating system is always a discovered operating system. Collected operating systems have a nonauthoritative status. You map nonauthoritative collected operating systems to normalized authoritative operating systems.

Normalized Operating System

A normalized operating system is always a *product-defined operating system*. Product-defined operating systems are collected from user input and other products that share the CA MDB. Product-defined operating systems always have an authoritative status. Authoritative status allows an operating system to have a normalization rule. You define a normalization rule for an authoritative normalized operating system when you map one or more collected operating systems to the authoritative operating system.

Subordinate Operating System

When you map a collected nonauthoritative operating system to a normalized authoritative operating system, the nonauthoritative operating system becomes subordinate to the authoritative operating system in the normalization rule.

Define Operating System Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can define operating system normalization rules that are applied during the matching process whenever the reconciliation rule contains asset matching criteria (see page 115). Any asset matching criterion that contains operating system information automatically applies the operating system normalization rules.

When you map a collected nonauthoritative operating system to a normalized authoritative operating system, the nonauthoritative operating system becomes subordinate to the authoritative operating system in the normalization rule. The subordinate operating system no longer appears in the Collected Operating System list. If you delete the normalization rule (see page 111) that contains the subordinate operating system, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list.

To define operating system normalization rules

1. Click Directory, List Management.
2. On the left, expand Normalization and select Operating System Normalization.

   The discovered Collected Operating System values and the Normalized Operating System values appear.
3. If the term you want to use as the normalized value does not appear in the Normalized Operating System list or the Collected Operating System list, click New Operating System to add the operating system, and then repeat the previous steps.
4. Map the Collected OS list discovered values to a Normalized OS value.

   The list of operating system normalization rules is defined and is referenced during the reconciliation process.

More information:

Operating System Normalization Rules (see page 106)

Update Operating System Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You update an operating system normalization rule when you want to change how a discovered operating system is normalized. This update may affect the value of the operating system in a matching asset. To update a normalization rule for an operating system, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change an operating system normalization rule and the reconciliation rule update option for operating system is enabled, the Hardware Reconciliation Engine changes the value of the operating system to the new normalized name in matching assets.

Important! If you change a normalization rule for an operating system that applies to public tenant data, the change may affect discovered assets for all tenants, depending on whether they use the specific operating system.

When you delete an operating system normalization rule, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list on the Normalization Rule page.

To update operating system normalization rules

1. Click Directory, List Management, Operating System Rules.
2. Delete the normalization rule (see page 111) that you want to change.
3. Define the new operating system normalization rule (see page 107).

More information:

Operating System Normalization Rules (see page 106)

System Model Normalization Rules

System model normalization rules are intended for hardware devices such as a computer, for example, Lenovo ThinkPad T400, Lenovo ThinkCentre M58, and so forth.

Collected System Model

A collected system model is always a discovered system model. Collected system models have a nonauthoritative status. You map nonauthoritative collected system models to normalized authoritative system models.

Normalized System Model

A normalized system model is always a *product-defined system model*. Product-defined system models are collected from user input and other products that share the CA MDB. Product-defined system models always have an authoritative status. Authoritative status allows a system model to have a normalization rule. You define a normalization rule for an authoritative normalized system model when you map one or more collected system models to the authoritative system model.

Subordinate System Model

When you map a collected nonauthoritative system model to a normalized authoritative system model, the nonauthoritative system model becomes subordinate to the authoritative system model in the normalization rule.

Define System Model Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can define system model normalization rules that are applied during the matching process whenever the reconciliation rule contains asset matching criteria (see page 115). Any asset matching criterion that contains system model information automatically applies the system model normalization rules.

When you map a collected nonauthoritative system model to a normalized authoritative system model, the nonauthoritative system model becomes subordinate to the authoritative system model in the normalization rule. The subordinate system model no longer appears in the Collected System Model list. If you delete the normalization rule (see page 111) that contains the subordinate system model, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list.

To define system model normalization rules

1. Click Directory, List Management.
2. On the left, expand Normalization and select System Model Normalization.

   The discovered collected system model name and manufacturer name values and the normalized system model name and manufacturer name values appear.
3. If the term you want to use as the normalized value does not appear in the Normalized System Model list or the Collected System Model list, click New System Model to add the system model, and then repeat the previous steps.
4. Map the Collected System Model list discovered values to a Normalized System Model value.

   The list of system model normalization rules is defined and is referenced during the reconciliation process.

More information:

System Model Normalization Rules (see page 109)

Update System Model Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You update a system model normalization rule when you want to change how a discovered system model is normalized. This update may affect the reconciliation process. To update a normalization rule for a system model, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change a normalization rule, the Hardware Reconciliation Engine processes assets so that the assets are matched using the new rule. Any assets that are matched as a result of a previous operation of the Hardware Reconciliation Engine are evaluated again to determine if their matching should change based on the new normalization rule.

When you delete a system model normalization rule, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list on the Normalization Rule page.

To update system model normalization rules

1. Click Directory, List Management, System Model Rules.
2. Delete the normalization rule (see page 111) that you want to change.
3. Define the new system model normalization rule (see page 109).

More information:

System Model Normalization Rules (see page 109)

View Normalization Rules

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can search for and view the normalization rules to see the mapping between collected values and the normalized values. This information is used during the hardware reconciliation process.

To view normalization rules

1. Click Directory, List Management.
2. On the left, expand Normalization and select the normalization rule type that you want to view.
3. Search for the normalized value or the collected value for which you want to view the normalization mapping rules.

   For each normalization rule, the collected value and its corresponding normalized value appear in the Search Results section.

Delete a Normalization Rule

Important! Normalization rules apply to all tenants and public data that are associated with a service provider. Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You delete a normalization rule when you no longer want asset matching criteria to apply the normalization rule during the reconciliation process or when you want to change a normalization rule. To change a normalization rule for a company, operating system, or system model, you delete the rule and define a new rule.

When you delete a company normalization rule, the subordinate company returns to nonauthoritative status and appears in the Collected Company list. If the subordinate company was a product-defined company, it also appears in the Normalized Company list on the normalization rule page. When you delete an operating system normalization rule, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list on the normalization rule page. When you delete a system model normalization rule, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list on the normalization rule page.

To delete a normalization rule

1. Click Directory, List Management.
2. On the left, expand Normalization and select the normalization rule type for the rule that you want to delete.
3. Search for the normalized value or the collected value for which you want to delete a normalization rule.

   For each normalization rule, the collected value and its corresponding normalized value appear in the Search Results section.
4. Select the rule that you want to delete.
5. Click Delete Rule.

   The normalization rule is deleted. Asset matching criteria do not apply the rule during the reconciliation process.

Updates to Normalization Rules

You update a system model or company normalization rule when you want to change how a discovered system model or company is normalized. This update may affect the reconciliation process. You update an operating system normalization rule when you want to change how a discovered operating system is normalized. This update may affect the value of the operating system in a matching asset. To update a normalization rule, you delete the rule and define a new rule.

The product monitors updates to normalization rules. If you change a system model or company normalization rule, the Hardware Reconciliation Engine performs the asset matching process so that the assets are matched using the new rule. Any assets that are matched as a result of a previous operation are evaluated again to determine if their matching should change based on the new normalization rule. If you change an operating system normalization rule, the Hardware Reconciliation Engine changes the value of the operating system to the new normalized name in matching assets if the reconciliation rule update option for operating system is enabled.

When you delete a company normalization rule, the subordinate company returns to nonauthoritative status and appears in the Collected Company list. If the subordinate company was a product-defined company, it also appears in the Normalized Company list on the Normalization Rule page. When you delete an operating system normalization rule, the subordinate operating system returns to nonauthoritative status and appears in the Collected Operating System list on the Normalization Rule page. When you delete a system model normalization rule, the subordinate system model returns to nonauthoritative status and appears in the Collected System Model list on the Normalization Rule page.

More information:

Define Company Normalization Rules (see page 104)
Define Operating System Normalization Rules (see page 107)
Define System Model Normalization Rules (see page 109)
Delete a Normalization Rule (see page 111)

Define a Reconciliation Rule

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

Use a reconciliation rule to define the processing options and actions that the Hardware Reconciliation Engine performs. You can define one reconciliation rule for each tenant.

Note: Each tenant can have only one reconciliation rule. Therefore, if you make a rule inactive, the inactive rule is the only reconciliation rule that is associated with the tenant. If you want to change the reconciliation rule for a tenant, you can update the current reconciliation rule (see page 123) or delete the current reconciliation rule (see page 124) and define a new rule. If you delete a rule, all asset matching links between discovered and owned assets that are associated with the rule are also deleted.

To define a reconciliation rule

1. Click Administration, Reconciliation Management.
2. On the left, click New Reconciliation Rule.
3. If applicable, select the tenant that is associated with the reconciliation rule that you are defining.
4. Enter the reconciliation rule information and click Save.

   Note: Select the Inactive check box if you want to suspend reconciliation processing for an individual tenant. If you select the Inactive check box, the Hardware Reconciliation Engine does not process the rule (no asset matching or data updates occur for the rule). For example, you can make a rule inactive temporarily while you define normalization rules or troubleshoot asset matching errors. If you make an existing rule inactive and the discovered and owned assets were already matched, the matching links are saved.

   The Monitor Asset Updates and Match Assets check boxes are available for selection.
5. (Optional) Select the Monitor Asset Updates check box to define the reconciliation update options (see page 114) that you want the Hardware Reconciliation Engine to update automatically.

   The Update Options pane opens.

6. (Optional) Select the Match Assets check box to define the asset matching criteria (see page 115) that you want the Hardware Reconciliation Engine to apply.

   The Matching Rules pane opens.

   Note: If you do not define matching criteria, the Hardware Reconciliation Engine uses the default asset matching criterion, which matches the owned serial number to the discovered serial number.

7. Click Save.

   The new reconciliation rule is defined.

Define Reconciliation Update Options

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can apply changes to selected, critical owned-asset fields when the Hardware Reconciliation Engine detects new values in the corresponding discovered-asset fields. The Hardware Reconciliation Engine monitors the critical fields that you select and updates the owned-asset fields when changes are detected in the corresponding discovered assets. You specify the owned-asset fields that you want to be automatically updated with changes that are found in the corresponding discovered assets.

To define reconciliation update options

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. Click the reconciliation rule for which you want to define reconciliation update options.
5. Select the Monitor Asset Updates check box to have the Hardware Reconciliation Engine apply automatic updates.

   The Update Options pane opens.

6. Select the check boxes for the fields that you want to be automatically updated.

   Note: Select the Host Name check box to enable and select the Copy Host Name to Asset Name update option.

7. Click Save.

   The new reconciliation update options are defined.

Asset Matching Criteria

The Hardware Reconciliation Engine matches the owned and discovered assets based on the *asset matching criteria* that you define for a reconciliation rule. The criteria define the matching factors for owned and discovered assets based on a list of field values from both CA APM and the discovery products. The Hardware Reconciliation Engine identifies all assets being managed and provides the required data during the reconciliation process.

If you modify the asset matching criteria associated with a reconciliation rule, the Hardware Reconciliation Engine reprocesses reconciled assets using the new criteria the next time the engine processes the rule.

You can match the following asset field values:

Owned Asset Field	Discovered Asset Field
Alternate Host Name	Host Name
Alternate Host Name	Registry Asset Name
Alternate ID	BIOS Asset Tag
Asset Alias	BIOS Asset Tag
Asset Alias	Host Name
Asset Name	Host Name
Class	System Type
Host Name	Host Name
Host Name	Registry Asset Name
MAC Address	MAC Address
MAC Address and Host Name	MAC Address and Host Name
Manufacturer	System Vendor
Model Name	System Model
Previous Asset Tag	BIOS Asset Tag
Serial Number	Serial Number
Subclass	System Type

The product monitors the asset matching fields of owned and discovered assets. If you modify the value of an owned asset field that can be used for asset matching, the Hardware Reconciliation Engine reprocesses the modified owned asset using the new value, during the next reconciliation process.

Similarly, if the discovery component of CA Client Automation or a third-party discovery product modifies the value of a discovered asset field in the CA MDB that can be used for asset matching, the Hardware Reconciliation Engine reprocesses the modified discovered asset using the new value, during the next reconciliation process.

The product also monitors changes to normalization rules for companies and system models. These rules affect the asset matching of owned and discovered assets. If you change one of the normalization rules, the Hardware Reconciliation Engine runs the asset matching process so that assets are matched using the new rules. Any assets that are matched as a result of a previous run of the Hardware Reconciliation Engine are evaluated again to determine if their matching should change based on the new normalization rules.

Inactive Status Effect on Asset Matching

Hardware Reconciliation processes all active owned assets created by CA APM that are not excluded from reconciliation (see page 118). An inactive asset, model, asset family, or company affects reconciliation links between owned and discovered assets as follows:

Inactive owned asset

- If an owned asset is inactive before the Hardware Reconciliation Engine matches the asset to a discovered asset, the owned asset is not matched.
- If an owned asset is made inactive after asset matching, the Hardware Reconciliation Engine clears the matching link the next time the engine processes the reconciliation rule.

Inactive Model

- When a model is made inactive before the Hardware Reconciliation Engine matches a discovered asset to an owned asset that is based on that model, the owned asset is not matched.
- When a model is made inactive after an owned asset that is based on that model is matched, the Hardware Reconciliation Engine clears the matching link for that asset and all others that are based on the inactive model the next time the engine processes the reconciliation rule.

Inactive Asset Family

- When an asset family, class, or subclass is made inactive before the Hardware Reconciliation Engine matches a discovered asset to an owned asset with that asset family, class, or subclass, the owned asset is not matched.
- When an asset family, class, or subclass is made inactive after an owned asset with the asset family, class, or subclass is matched, the Hardware Reconciliation Engine clears the matching link for that asset and all others that belong to the inactive asset family, class, or subclass the next time the engine processes the reconciliation rule.

Inactive Company

- When a company is made inactive before the Hardware Reconciliation Engine matches a discovered asset to an owned asset with that company as the manufacturer, the owned asset is not matched.
- When a company is made inactive after an owned asset with that company as the manufacturer is matched, the Hardware Reconciliation Engine clears the matching link for that asset and all others that are associated with the inactive company the next time the engine processes the reconciliation rule.

Note: For more information about making assets, models, asset families, and companies inactive, see the *User Guide*.

More information:

Exclude an Asset Family from the Reconciliation Process (see page 119)

Define Asset Matching Criteria

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

Based on the matching criteria that you define for a reconciliation rule, the product attempts to match the owned and discovered assets. The Hardware Reconciliation Engine performs the asset reconciliation when the ownership field value matches the discovered field value.

To define asset matching criteria

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. Click the reconciliation rule for which you want to define an asset matching criterion.

   The Reconciliation Rule Details page opens.

5. Select the Match Assets check box to have the Hardware Reconciliation Engine apply asset matching criteria.

   The Matching Rules pane opens.

6. Select the owned and discovered fields that you want to match and click Add Criteria.

   A new asset matching criteria record is added to the Matching Criteria section and a new trimming record is added to the Trimming section.

7. Click the Edit Record icon next to the new criterion in the Matching Criteria section.

8. Select the matching criterion options.

9. (Optional) In the Trimming section, click the Edit Record icon and select trimming options for the asset matching criterion. For example, discovered computer names at one site have a three-character location code as a prefix, which is not in the owned asset computer name. You create a trimming record for the asset matching criterion that trims three characters from the left side of the discovered computer names.

10. (Optional) Continue to add matching criteria to the reconciliation rule.

11. Click Save.

    The new asset matching criteria are defined and the reconciliation rule is saved.

Note: After a reconciliation rule is saved, if you want to change the matched fields in an asset matching criterion to different fields, delete the criterion and create a new one.

Exclude an Ownership Asset from the Reconciliation Process

You can exclude individual owned assets from the reconciliation process. Some reasons for excluding assets from reconciliation include the following examples:

- An owned asset has no matching discovered asset and continues to be included in the list of unreconciled assets. For example, assets that are never attached to the network, like some laptops, or assets that are retired, but their ownership data is stored in CA APM.
- A company does not want to include a particular class of asset, for example, laptops, in reconciliation.

If an owned asset is excluded from the reconciliation process before the Hardware Reconciliation Engine matches the asset to a discovered asset, the owned asset is not available for matching. If an owned asset is excluded from the reconciliation process after asset matching, the Hardware Reconciliation Engine clears the matching link the next time the engine processes the reconciliation rule. The owned asset is not available for matching.

Note: If the asset family of an excluded asset is set to be included in the hardware reconciliation process, the asset continues to be excluded from the process. If an asset family is excluded from the hardware reconciliation process (see page 119), all assets that belong to the excluded asset family are excluded.

To exclude an ownership asset from the reconciliation process

1. Click Asset, Asset Search.
2. Search to find the list of available assets.
3. Click the asset that you want to exclude from the reconciliation process.
4. In the Basic Information section, select the Exclude Reconciliation check box.
5. Click Save.

   The ownership asset is not included in future reconciliations.

More information:

Inactive Status Effect on Asset Matching (see page 116)

Exclude an Asset Family from the Reconciliation Process

You can exclude all owned assets in an asset family from the hardware reconciliation process. Some reasons for excluding asset families from reconciliation include the following examples:

- Assets in an asset family have no matching discovered assets and continue to be included in the list of unreconciled assets. For example, assets that are in the service asset family are not attached to the network, but their ownership data is stored in CA APM.
- The asset family is software. The product does not reconcile software.
- A company wants to make an asset family inactive. Hardware Reconciliation processes active owned assets created by CA APM.

If an asset family is excluded from the reconciliation process before the Hardware Reconciliation Engine matches owned assets in that asset family to discovered assets, the owned assets are not available for matching. If an asset family is excluded from the reconciliation process after owned assets in that asset family are matched, the Hardware Reconciliation Engine clears the matching links the next time the engine processes the reconciliation rule. The owned assets are not available for matching.

To exclude an asset family from the reconciliation process

1. Click Directory, List Management.
2. On the left, expand Asset Lists and click Asset Family.
3. Click the Edit Record icon for the asset family that you want to exclude from the reconciliation process.
4. Complete one of the following options:
   - Clear the Reconcile Hardware check box.
   - Select the Is Software check box.
   - Select the Inactive check box.
5. Select the Complete Record Edit icon for the asset family object.
6. Click Save.

   Assets in the excluded asset family are not included in future reconciliations.

Exclude an Asset Family Class or Subclass from the Reconciliation Process

You can exclude all owned assets in an asset family class or subclass from the hardware reconciliation process. For example, you can exclude assets because your company wants to make an asset family class or subclass inactive. Hardware Reconciliation processes active owned assets created by CA APM.

If an asset family class or subclass is excluded from the reconciliation process before the Hardware Reconciliation Engine matches discovered assets to owned assets in that asset family class or subclass, the owned assets are not available for matching. If an asset family class or subclass is excluded from the reconciliation process after owned assets in that asset family class or subclass are matched, the Hardware Reconciliation Engine clears the matching links the next time the engine processes the reconciliation rule. The owned assets are not available for matching.

To exclude an asset family class or subclass from the reconciliation process

1. Click Directory, List Management.
2. On the left, expand Asset Lists and click Asset Family.

3. Click the Edit Record icon for the asset family with a class or subclass you want to exclude from the reconciliation process.
4. Click Class List.
5. Click the Edit Record icon for the class you want to exclude from the reconciliation process (or the class with a subclass you want to exclude).
6. Select the Inactive check box and click the Complete Record Edit icon for the asset family class if you want to exclude the entire class.

   Note: Skip this step if you want to exclude a subclass, but not the entire class, from the reconciliation process.
7. Click Subclass List if you want to exclude a subclass.
8. Click the Edit Record icon for the subclass you want to exclude from the reconciliation process.
9. Select the Inactive check box and click the Complete Record Edit icon for the asset family subclass.
10. Click Save.

    Assets in the excluded asset family class or subclass are not included in future reconciliations.

View the Reconciliation Results

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

When the Hardware Reconciliation Engine processes actions for a reconciliation rule, the engine writes records to the message queue in the database. You can search the message queue for reconciliation log messages. The message queue retains log messages for a configurable number of days.

Note: You can control the level of detail written to the message queue by changing the Hardware Reconciliation Engine logging level. You can also control the number of days that messages are retained in the message queue. For more information about logging level and message queue retention settings, see Hardware Reconciliation Engine Configuration Settings (see page 136).

To view the message queue

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Message Search.

   The message queue displays reconciliation log messages in the Search Results section.

3. (Optional) Search to find a message in the message queue.

Note: You can export the message queue to a comma-separated values (CSV) file for use in a spreadsheet application. You can also generate reports to view information about your environment relative to reconciliation. For more information about generating reports, see the *User Guide*.

Add Assets from Unreconciled Discovered Records

The hardware reconciliation process can detect assets that cannot be reconciled with any of your owned assets. You can decide to add the unreconciled assets to your repository so that you can track and manage all assets in your network. You can add the unreconciled assets by generating and exporting the results of a report and then importing the report results through the Data Importer.

Important! Before you import data into CA APM, review the data to ensure accuracy and uniqueness.

To add assets from unreconciled discovered records

1. Log in to BusinessObjects Enterprise InfoView.

   The Reports pane opens.

2. Click Document List.

3. Expand Public Folders, CA Reports.

4. Click CA ITAM.

5. Double-click the icon to the left of the report that identifies the discovered assets that are not matched to any owned assets.

6. Enter the search criteria for the report.

   Note: Select one tenant only when you generate the report. You can import data into only one tenant at a time.

7. Click Run Query.

8. Click the link for the flat file format that you can export.

   The report is converted to a document format that you can view and export.

9. Save the document as a CSV file.

10. Log in to CA APM as the administrator.

11. Navigate to Administration, Data Importer, New Import.

12. Specify the CSV file name in the Data File field.
13. Select the main destination object and the delimiter.

    Important! Select the same tenant that you selected when you generated the report.

14. In the Advanced Settings area, verify that the following options are selected:
    - Insert or Update
    - Create Secondary Lookup Object
    - Update Secondary Lookup objects
    - Error on Secondary Lookup Object Errors
15. Click Save.
16. Specify the column mapping.
17. Click Submit in the Schedule area to start the import process.

    The unreconciled assets are added to your data repository.

Update a Reconciliation Rule

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can update the information for a reconciliation rule.

If you modify the asset matching criteria associated with a reconciliation rule, the Hardware Reconciliation Engine reprocesses reconciled assets using the new criteria the next time the engine processes the rule.

To update a reconciliation rule

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. Click the reconciliation rule that you want to update.

5. Enter the new information for the reconciliation rule.

   Note: Select the Inactive check box if you want to suspend reconciliation processing for an individual tenant. If you select the Inactive check box, the Hardware Reconciliation Engine does not process the rule (no asset matching or data updates occur for the rule). For example, you can make a rule inactive temporarily while you define normalization rules or troubleshoot asset matching errors. If you make an existing rule inactive and the discovered and owned assets were already matched, the matching links are saved.

6. Click Save.

   The reconciliation rule is updated.

Note: After a reconciliation rule is saved, if you want to change the matched fields in an asset matching criterion to different fields, delete the criterion and create a new one.

Delete a Reconciliation Rule

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

You can delete a defined reconciliation rule. If you delete a rule, all asset matching links between discovered and owned assets that are associated with the rule are also deleted.

Each tenant can have only one reconciliation rule. If you want to change the reconciliation rule for a tenant, update the current reconciliation rule (see page 123) or delete the current rule and define a new reconciliation rule (see page 113).

Note: You can also make a rule inactive if you want to suspend reconciliation processing temporarily for an individual tenant. To make a rule inactive, update the rule (see page 123) and select the Inactive check box. If the discovered and owned assets were already matched for the rule, the matching links are saved.

To delete a reconciliation rule

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Rule Search.
3. Search to find the list of available reconciliation rules.
4. Click the rule that you want to delete.
5. Click Delete and confirm that you want to delete the reconciliation rule.

   The rule is deleted.

Export the Reconciliation Results

Important! Verify that the user completing this task belongs to a role in which reconciliation management access is enabled (see page 16).

After you view the message queue, you can export the queue to a comma-separated value (CSV) file for use in a spreadsheet application.

To export the message queue

1. Click Administration, Reconciliation Management.
2. On the left, click Reconciliation Message Search.

   The message queue displays reconciliation log messages in the Search Results section.
3. Search to find the reconciliation log messages that you want to export.
4. Click Export to CSV.

   The message queue search results are exported to a CSV file and a link to the CSV file appears.

Chapter 5: Managing Product Components

This section contains the following topics:

Product Components

After you install CA APM, you can manually configure many of the product components. In addition, you can add components to additional servers to maintain optimum performance and enable scalability. For example, you can add a Hardware Reconciliation Engine or an additional component server. The configuration is flexible, and you can change many component settings.

Note: For a description of each product component, see the *Implementation Guide*.

Configure a Product Component

Important! Verify that the user completing this task belongs to a role in which system configuration access is enabled (see page 16).

You can change the component configurations that were set up during the product installation. For example, you can change the name of the SMTP server that is used to send email.

Follow these steps:

1. Click Administration, System Configuration.
2. On the left, select the product component.
3. Enter the new configuration settings for the component:
   - Database
     - Oracle (see page 128)
     - SQL Server (see page 130)
   - Web Server (see page 132)
   - Application Server (see page 135)
   - Hardware Reconciliation Engine (see page 136)

- CA EEM (see page 137)
- Export Service (see page 138)
- Data Importer (see page 139)
- Data Importer Engine (see page 140)
- LDAP Data Import and Sync Service (see page 141)
- CORA (see page 141)
- Storage Manager Service (see page 142)
- Event Service (see page 142)
- Common Asset Viewer (see page 145)
- WCF Service (see page 146)
- SAM - Import Driver (see page 147)
- Software Asset Management (see page 147)

4. Click Save.

   The configuration settings are saved.

Oracle Database Configuration Settings

After you install the product, if you are using Oracle as the database for the CA MDB, you can change the settings for the Oracle database server.

The following fields require explanation:

DBA User Name

The user name for connecting to the target database. The user name must be for a privileged user.

Default: sys

Listen Port

The database connection port.

Default: 1521

Oracle Service Name

The service name for the target database.

Default: orcl

Oracle Net Service Name

The net service name for the target database.

Default: orcl

Tablespace Path

The location of the Oracle tablespaces.

Default: c:\oracle\product\10.2.0\oradata\orcl

Data Tablespace Name

The name of the data tablespace.

Default: MDB_DATA

Data Tablespace Size

The amount of disk space to be allocated for the data tablespace.

Default: 400 MB

Index Tablespace Name

The name of the index tablespace.

Default: MDB_INDEX

Index Tablespace Size

The amount of disk space to be allocated for the index tablespace.

Default: 100 MB

mdbadmin Password

The password that is associated with the mdbadmin user. If a new CA MDB is being created, this is the password that is assigned to the mdbadmin user.

Command Timeout

The maximum amount of time that the application waits for a response from the database.

Stored Procedure Command Timeout

The maximum amount of time that the application waits for a response from the database stored procedures.

Max Connection Pool Size

The maximum number of requests that the database can process simultaneously.

Enable CORA Connection Pooling

Placeholder for the flag that enables CORA connection pooling. Currently, CORA does not support connection pooling.

CORA Connection Pool Lifetime

Placeholder for the lifetime of the CORA connection pool. Currently, CORA does not support connection pooling.

CORA Connection Pool Size

Placeholder for the size of the CORA connection pool. Currently, CORA does not support connection pooling.

Last Run Date Option

Determines if the imported data should update the existing CA APM data.

Note: CA APM receives discovered hardware data imports and uses the data to match ownership and discovery data. CA APM determines if the imported data is more current than the existing data by comparing their inventory dates. Then CA APM decides whether the imported data should update the existing CA APM data.

Default: 2

Note: See the following table for a description of all valid options.

Option	Definition
1	Always update the existing CA APM data with the imported data.
2	(Default) Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, an error occurs and the imported asset data does not update the existing CA APM data.
3	Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, update the existing CA APM data with the imported data.

SQL Server Database Configuration Settings

After you install the product, if you are using SQL Server as the database for the CA MDB, you can change the settings for the SQL Server database server.

The following fields require explanation:

SQL Server Login

The user name for connecting to the target database. The user name must have sysadmin role privileges assigned in SQL Server.

Default: sa

SQL Server TCP/IP Port

The database connection port.

Default: 1433

Command Timeout

The maximum amount of time that the product waits for a response from the database.

Stored Procedure Command Timeout

The maximum amount of time that the product waits for a response from the database stored procedures.

Max Connection Pool Size

The maximum number of requests that the database can process simultaneously.

Enable CORA Connection Pooling

Placeholder for the flag that enables CORA connection pooling. Currently, CORA does not support connection pooling.

CORA Connection Pool Lifetime

Placeholder for the lifetime of the CORA connection pool. Currently, CORA does not support connection pooling.

CORA Connection Pool Size

Placeholder for the size of the CORA connection pool. Currently, CORA does not support connection pooling.

SQL Server Host Name

The host name of the server that is used for SQL Server.

Last Run Date Option

Determines if the imported data should update the existing CA APM data.

Note: CA APM receives discovered hardware data imports and uses the data to match ownership and discovery data. CA APM determines if the imported data is more current than the existing data by comparing their inventory dates. Then CA APM decides whether the imported data should update the existing CA APM data.

Default: 2

Note: See the following table for a description of all valid options.

Option	Definition
1	Always update the existing CA APM data with the imported data.
2	(Default) Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, an error occurs and the imported asset data does not update the existing CA APM data.
3	Update the existing CA APM data only if the inventory date of the imported asset is more current than the inventory date of the existing asset. If the imported asset does not have an inventory date, update the existing CA APM data with the imported data.

Web Server Configuration Settings

After you install the product, you can change the settings for the web 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.

Authentication Timeout

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the product and must log in again.

Default: 3600000 (6 minutes)

State Data

The temporary view data that is stored at the server side for each user until the user logs off. This data can be stored either in the database or on the web server file system. The value of State Data can be SERVER (FileSystem) or DATABASE.

Cache Timeout

The elapsed time-out period for cached files to be deleted from the store.

When a user logs in, along with view data, documents are stored in system memory (Cache). If the user is not referring to these documents, the documents become stale. After some time, these documents are deleted. The time limit is the Cache Timeout.

Auto complete Result Count

The number of values to display in the Auto Complete drop-down lists. In fields with lists, the user can start to type a value and the product provides a list of matching values. The user can then select a value from this Auto Complete list.

Note: If you set a low number for this parameter, the Auto Complete list may not be useful since the user will have to type most of the value before finding it in the list. If you set a high number for this parameter, the list could perform slowly.

Homepage

The default CA APM home page that is opened after the user logs in.

SM Web Service Protocol

The protocol that is used to access the Storage Manager Service.

The Storage Manager Service provides file storage facility to other product components. When the other components want to interact with the Storage Manager Service, the components use this protocol.

SM Web Service Port

The port on which the Storage Manager Service is running.

This port is the HTTP port on which the Storage Manager Service is hosted. The default port is 80. If the Storage Manager Service is configured to host on a different port, that port number is shown.

EEM Backend

The name of the server where CA EEM is installed. This value is populated during installation.

Reporting Web Service Server

The CA Business Intelligence server name and port. This value is populated during installation.

Reporting Timeout

The time-out in seconds for a connection to the CA Business Intelligence (reporting) web service.

Reporting Name

The name of the CA Business Intelligence (reporting) engine. This name is always "Allegheny Reporting Engine".

Reporting User

The CA Business Intelligence (reporting) user with administrative privileges.

Reporting Password

The password for the Reporting User.

External AuthHeader

This header works with the External setting of Authentication Type on the CA EEM configuration. The external authentication mechanism sets information in the HTTP header for the CA APM web pages to receive. One piece of information is the User Id. The External AuthHeader is the name of the variable external authentication that sets the User Id value. The External AuthHeader setting must match the configured setting in the external authentication for which the User Id is provided.

From Address

The From email address for the notifications that are sent from the Event Service.

To List

The list of recipients who receive the email notifications about issues from the Event Service.

Cc List

The list of recipients in the Cc list who receive the email notifications about issues from the Event Service.

Bcc List

The list of recipients in the Bcc list who receive the email notifications about issues from the Event Service.

Email Subject

The subject line in the email notification about issues that the Event Service sends to the recipients in the To List, Cc List, and Bcc List.

Note: If you change the setting on Administration, System Configuration, Web Server for the Web Server Protocol or the Web Server or Load Balancer IP/Host, you must restart the Windows service for CA Asset Portfolio Management – Export Service.

Application Server Configuration Settings

After you install the product, you can change the settings for the application 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.

Authentication Timeout

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the product and must log in again.

Default: 3600000 (6 minutes)

EEM Backend

The name of the server where CA EEM is installed. This value is populated during installation.

USM Web Service URL

The URL for the USM web service. This value is used when the product is integrated with CA Service Catalog or CA Service Desk Manager.

Note: If you change the setting on Administration, System Configuration, Application Server for the Web Service Protocol or the Application Server or Load Balancer IP/Host, you must restart the following Windows services:

- CA Asset Portfolio Management – Export Service
- CA Asset Portfolio Management – Event Service
- CA Asset Portfolio Management – HW Reconciliation Engine
- CA Asset Portfolio Management – LDAP Import Service

Hardware Reconciliation Engine Configuration Settings

After you install the product, you can change the settings for the Hardware Reconciliation Engine.

The following fields require explanation:

Message Queue Retention

Number of days that records remain in the message queue before the Hardware Reconciliation Engine purges them.

Default: 7

Refresh Lock Record Count

Engine performance tuning setting that works with the Lock Stale Interval setting. The number of records that the Hardware Reconciliation Engine adds or updates before refreshing the lock on the reconciliation rule record. If the lock refresh does not happen within the number of seconds specified in the Lock Stale Interval setting, the reconciliation rule record is available to another Hardware Reconciliation Engine.

Default: 100

Lock Stale Interval

Engine performance tuning setting that works with the Refresh Lock Record Count setting. If the lock refresh does not happen on the reconciliation rule, the amount of time, in seconds, after which a reconciliation rule record is available to another Hardware Reconciliation Engine.

Default: 600

Web Service Authentication Timeout

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the service and must log in again.

Default: 3600000 (6 minutes)

Processing Mode

Specifies whether the Hardware Reconciliation Engine processes continuously. The product supports the following option:

0

Process in continuous reconciliation mode.

Engine Snooze Time

Amount of time, in milliseconds, that the Hardware Reconciliation Engine waits between processing cycles.

Default: 300000 (5 minutes)

Connection Retry Time

Amount of time, in milliseconds, that the Hardware Reconciliation Engine waits between attempts to connect to the database.

Default: 60000 (1 minute)

Engine Debug Level

Debug level for the message queue. The levels are Fatal, Error, Warning, Info, and Debug.

Default: Fatal

Web Service Batch Size

Number of records that are sent to the web service at one time for update processing.

Default: 50

Pending Modification Retention

Number of days that pending modification requests remain in the queue before the Hardware Reconciliation Engine purges them. This setting affects any tenant that is processed by the Hardware Reconciliation Engine.

Default: 7

More information:

Hardware Reconciliation Engine (see page 100)

CA EEM Configuration Settings

After you install the product, you can change the settings for CA EEM.

The following fields require explanation:

Authentication Type

Type of authentication allowed:

- **Form**. A user is prompted for a user name and password to log in to the product.
- **Windows Integrated**. A user who is already logged in to the Windows domain can access the product without having to provide additional login credentials.
- **External**. A user is authenticated by an external access management system, for example, CA SiteMinder.

Default: Form

uapmadmin Password

Password for the uapmadmin user to access the web and application servers.

Export Service Configuration Settings

After you install the product, you can change the settings for the Export Service.

The following fields require explanation:

On Demand Request Period

Amount of time, in milliseconds, that the Export Service waits between On Demand Request processing cycles.

Default: 5000 (5 seconds)

On Demand Maximum Threads

Number of On Demand Request processing threads.

Default: 2

Scheduled Requests Period

Frequency, in milliseconds, of Scheduled Requests processing cycles.

Default: 7200000 (2 hours)

SMTP Server

Email server name.

Authentication Timeout

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the product and must log in again.

Default: 360000 (6 minutes)

Purge Start Time

Time of day, in 24-hour format (Universal Time) when the purge thread starts.

Default: 5 (5:00 a.m. Universal Time)

Search Batch Size

Maximum number of data records returned for each search in a single export request. Changing the default value may affect performance. For example, a lower value may increase the number of web service calls that are needed to retrieve all the data, and a higher value may require a longer period of time to gather all the records.

Default: 2000

SM Web Service Protocol

The protocol that is used to access the Storage Manager Service.

SM Web Service Port

The port on which the Storage Manager Service is running.

Export Service Email Address

The email address that is used by the Export Service for notifications.

Data Importer Configuration Settings

After you install the product, you can change the settings for the Data Importer.

The following fields require explanation:

Authentication Timeout

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the component and must log in again.

Default: 3600000 (6 minutes)

Maximum Batch Record Size

Maximum number of records in a Data Importer batch.

Default: 50

Data Importer Engine Configuration Settings

After you install the product, you can change the settings for the Data Importer Engine.

The following fields require explanation:

SMTP Server Value

The email server name.

Scheduled Requests Period

The amount of time that the Data Importer Engine waits before checking for pending scheduled import requests. This value applies to scheduled data imports only.

Default: 60000 (60 seconds)

On Demand Request Period

The amount of time that the Data Importer Engine waits before checking for pending on demand import requests. This value applies to on demand data imports only.

Default: 60000 (60 seconds)

Max Batch Record Size

Maximum number of records in a Data Importer Engine batch.

Default: 100

Max Job Threads

The maximum number of Data Importer Engine threads that can be running simultaneously for one import job.

Default: 5

Max Import Threads

The maximum number of Data Importer Engine threads that can be running simultaneously for all import jobs.

Default: 5

LDAP Data Import and Sync Service Configuration Settings

After you install the product, you can change the settings for the LDAP Data Import and Sync Service.

The following fields require explanation:

DB Check Time

Amount of time, in milliseconds, that the service checks the status (active or sleep mode). If the status is active, the service starts importing data.

EEM Backend

The name of the server where CA EEM is installed. This value is populated during installation.

CORA Configuration Settings

After you install the product, you can change the settings for CORA (CA APM Registration Service).

The following fields require explanation:

Note: Changes to the Common parameters affect the Web Server, WCF Service, Hardware Reconciliation, and Application Server components. Changes to the Registration Service parameters affect the Registration Service component.

(Common) Enable CORA

Enables Common Object Registration API features for the Web Server, WCF Service, Hardware Reconciliation, and Application Server components.

Default: False

(Common) Enable CORA ID Generation

Allows the CORA tables to get the next CORA ID for a new record for the Web Server, WCF Service, Hardware Reconciliation, and Application Server components.

Default: True

(Registration Service) Enable CORA

Enables the Common Object Registration API features using the Registration Service for all CA APM components.

Default: True

(Registration Service) Enable CORA ID Generation

Allows the CORA tables to get the next CORA ID for a new record using the Registration Service for all CA APM components.

Default: False

Storage Manager Service Configuration Settings

After you install the product, you can change the settings for the Storage Manager Service.

The following fields require explanation:

Purge Start Time

Time of day, in 24-hour format, when the Storage Manager Service starts to delete unused files.

Authentication Timeout

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the service and must log in again.

Default: 3600000 (6 minutes)

Event Service Configuration Settings

After you install the product, you can change the settings for the Event Service.

The following fields require explanation:

Provider URL

The URL for accessing the workflow provider (for example, CA Process Automation).

Example: The following URL is the default CA Process Automation workflow web services URL:

`http://<wf_hostname>:<wf_tomcat_port>/itpam/soap`

Provider Authentication Type

The type of authentication (user or CA EEM) to be used with the Event Service.

Default: User (CA EEM authentication is not currently supported for the Event Service.)

Provider User Name

The user ID for logging in to the workflow provider.

Provider Password

The user password for logging in to the workflow provider.

Provider Process Path

The path for accessing the start request forms for the workflow provider. These forms must be available for the CA APM integration with the workflow provider. For more information, see your workflow provider documentation.

Default: /

Number of Events to be Processed

The maximum number of events to be processed in one Web Service call.

Default: 2000

Time of the day for Event purge (in hours, GMT)

The time of day, in 24-hour format (GMT), when CA APM starts to purge event definitions that are marked for deletion.

Default: 5 (5:00 a.m. GMT)

CMDB Audit Share Required

The indicator that enables audit sharing with the CMDB.

The CMDB common database tables can be used by multiple applications. For example, the ca_contact table is used by CA APM, CA Service Catalog, and CA Service Desk Manager when they are integrated. An audit table maintains the changes that are made to these common tables. When there is a change to any of the CMDB objects in CA APM and this value is set to true, the change audit is posted to the CMDB audit table.

From Address

The From email address for the notifications that are sent from the Event Service.

To List

The list of recipients who receive the email notifications about issues from the Event Service.

Cc List

The list of recipients in the Cc list who receive the email notifications about issues from the Event Service.

Bcc List

The list of recipients in the Bcc list who receive the email notifications about issues from the Event Service.

Email Subject

The subject line in the email notification about issues that the Event Service sends to the recipients in the To List, Cc List, and Bcc List.

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.

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

Common Asset Viewer

After you install the product, you can change the settings for the 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.

The following fields require explanation:

Tomcat Port

Port that should be used for the Apache Tomcat server that is processing the Common Asset Viewer.

Default: 9080

Note: You must first update the port in the Apache Tomcat configuration file before you change the setting in the product. For information about updating the Apache Tomcat configuration file, see the *Implementation Guide*.

WCF Service Configuration Settings

After you install the product, you can change the settings for the Windows Communications Foundation (WCF) Service component.

The following fields require explanation:

WCF Service Load Balancer IP/Host

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

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

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

Authentication Timeout (in milliseconds)

Amount of time, in milliseconds, that users can be inactive before they are automatically logged out of the service and must log in again.

Default: 3600000 (6 minutes)

Operation Threshold

The maximum number of records that can be sent by or returned to the client or server. When you call the Search method from a WCF client program, this value represents the maximum number of records that can be returned to you. If you call the Create method, this value represents the maximum number of records that you can send at one time.

EEM Backend

The name of the server where CA EEM is installed. This value is populated during installation.

SAM - Import Driver Configuration Settings

After you install the product, you can change the settings for the CA SAM Import Driver.

The following fields require explanation:

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

Data Importer Executable Path

The path to the Data Importer executable file (ITAM Data Importer.exe).

Example: *[ITAM Root Path]*\ITAM\Data Importer\ITAM Data Importer.exe

CA SAM Server Name

The name of the server where CA SAM is installed.

Software Asset Management Configuration Settings

After you install the product, you can configure the settings for software asset management. After you configure these settings, 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

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.

Add Component Servers

Important! Verify that the user completing this task belongs to a role in which system configuration access is enabled (see page 16).

After the product is installed, you can add components to additional servers to maintain optimum performance and enable scalability as your enterprise grows. You can install the following components on one or more servers:

- Web server
- Application server
- Hardware Reconciliation Engine
- Data Importer
- WCF
- Data Importer Engine

To add a product component server

1. Click Administration, System Configuration.
2. On the left, select the product component.
3. Specify the required server connection information in the Add Component to Server section, including the administrator username and password for the server.
4. Click Add.

   The server is added to the Component Server List.
5. Enter the configuration settings for the new component server:
   - Web Server
   - Application Server
   - Hardware Engine
   - Data Importer
6. Click Save.

   The configuration settings for the component are saved for the new server.

   Note: Install CA APM on the server you just added. For information about installing, see the *Implementation Guide.*

Modify the Debugging Level for Component Service Log Files

The product components have corresponding Windows services. These services create log files that allow you to verify the service status and review error details. The amount of detail information in a log file depends on the specified debugging level. The default debugging level for the service log files is Fatal. You can change the default level for the Windows services by editing the log configuration file for each component.

Follow these steps:

1. Navigate to a component folder on the application server where CA APM is installed.

   Example:

   [ITAM Root Path]\ITAM\Hardware Engine

2. Open the logging.config file in a text editor (for example, Notepad).
3. Locate the debugging level value statements.
4. Edit the statements to include your debugging levels.

   Note: The log configuration files contain comments that explain the different debugging level values.

5. Save the log configuration file.

Chapter 6: How to Secure CA APM Data with Filters

This section contains the following topics:

How to Secure CA APM Data with Filters

You can set up CA APM data security by creating data filters. You use the data filters to limit the data that users and user roles can view, create, or modify. Users can view, create, or modify only the data that the filter specifies. You can create filters for any of the primary objects:

- Asset
- Model
- Legal Document
- Contact
- Company
- Location
- Organization
- Site

  Note: You cannot create a filter for a secondary object that is included in List Management. For example, you can filter assets (primary object) based on the cost center (secondary object) so that you only see assets that belong to a specific cost center. However, all cost centers are still accessible. To restrict access to cost centers (or other secondary objects), assign the user to a configuration that does not allow access to these objects.

As a system administrator, you define filters that limit data access in the following ways:

- Limit data based on the current user (contact).

  For example, define a filter that limits assets by the cost center of the contact. If you apply the filter to all users, the assets dynamically filter based on each user cost center. If the contact cost center is changed, the product filters the assets for the new cost center automatically.

- Limit data based on fixed values.

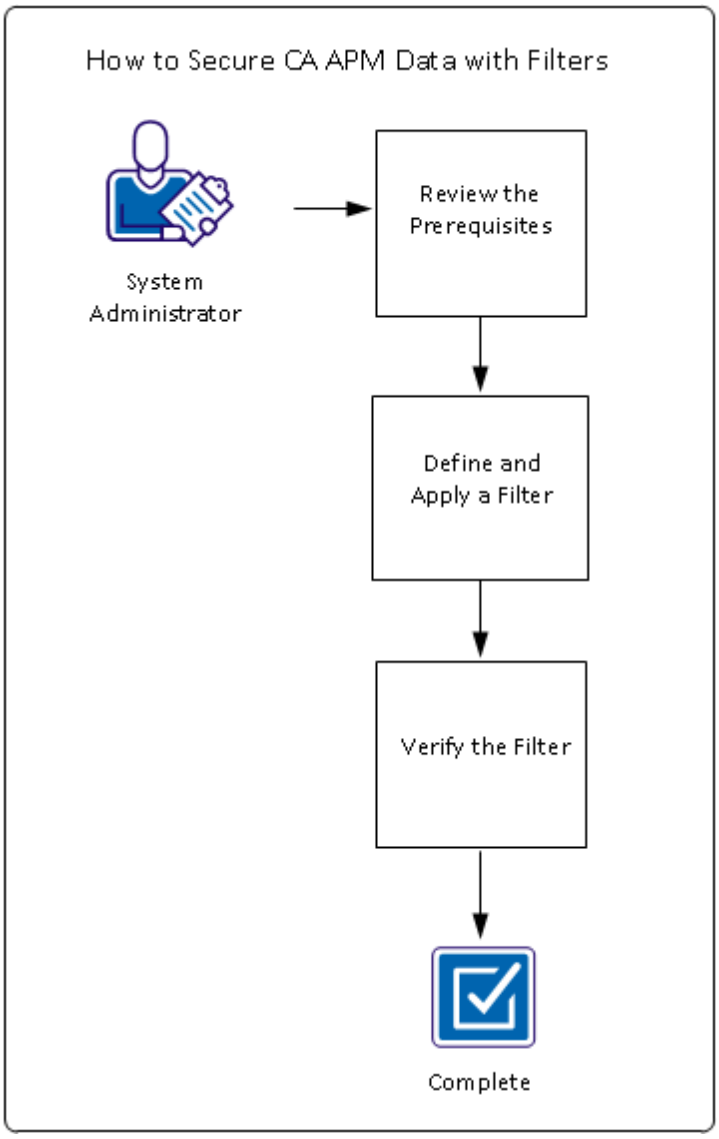
  For example, allow a user to view assets in the Development cost center. Development is a fixed value. If the cost center changes, the cost center is not automatically changed in the filter.

The data that matches the filter criteria is accessible to filter users.

Note: You can also set up CA APM security by configuring the user interface. Through this configuration, you can control user access to the different functions in CA APM.

Important! In this scenario, the system administrator defines the filters. However, the administrator can grant filter management permissions to any CA APM user role.

The following diagram illustrates how a system administrator secures CA APM data with filters.



To filter CA APM data, perform these steps:

1. Review the Prerequisites (see page 156).
2. Define and Apply a Filter (see page 156).
3. Verify the Filter (see page 159).

Example: Filter Asset Data by Cost Center

Sam, the CA APM system administrator at Document Management Company, wants to ensure that organizational data security requirements are met. Sam wants to limit user access to the company asset records so that users see only their own cost center data. Sam creates a filter for Asset (All Families) and assigns the filter to particular users. Sam verifies that the filter works to ensure the organizational data security.

Review the Prerequisites

To ensure that you can successfully filter data, verify that you have completed the following prerequisites:

1. Identify the product data that you want to limit by user or role.
2. Identify the users and roles that have limited data access.

Define and Apply a Filter

Define a filter and assign the filter to a role, a user, or a combination of roles and users. The product displays only the data that the user is authorized to access.

Follow these steps:

1. Click Administration, Filter Management.
2. On the left, click New Filter.
3. In the Filter Information area, enter the required and optional (if needed) information. The following fields require explanation:

   Object

   Specifies the object data that you want to filter. The object that you select determines the fields that you can use as criteria in the Filter Criteria area.

   Note: If you select Model or Asset, select a family, also. If you select Legal Document, select a template, also. The filter is applied to objects that belong to the family or template that you select. For example, a filter for the hardware asset object does not apply to any other asset family.

   Important! You cannot change the object or the object family or template after you specify filter criteria or after you save the filter. Delete the filter criteria to change the object.

   Family or Legal Template

   Specifies the family for the Model or Asset object or specifies the template for the Legal Document object.

4. In the Filter Security area, enter information for role or user security.

   Important! If you save your filter without selecting a user or role in the Filter Security area, your filter is not applied to any users.

5. In the Filter Criteria area, click Add Fields.
6. Select a field from the dialog and click OK.

   The criterion is shown in the Filter Criteria list.

7. Click the Edit Record icon next to the criterion you added.
8. Enter information to define the filter criterion for a selected field. The following fields require explanation:

   Left Parenthesis

   Specifies the first criterion in a group of criteria. You can define groups of criteria to control the logic of the filter.

   Note: If you select Left Parenthesis to define the first criterion in a group, select Right Parenthesis for the last criterion in the group.

   For example, you can filter for assets with the asset name OE001 or with both the asset family Computer and the asset name Dell. In this example, the group consists of two criteria. The Left Parenthesis is selected for the first criterion, which states that the asset family is Computer. The Right Parenthesis is selected for the second criterion, which states that the asset name is Dell.

   Field Name

   Specifies the field data that is filtered.

   Operator

   Specifies the filter operator to use to filter object data. For all operators except Has Value and Has No Value, enter a value in the Value field.

   For example, you can filter assets in which the asset name is not equal to OE001 and the asset family is equal to Computer.

   Note: If you specify an Operator and Value, the filter limits data based on a fixed value for the Field Name. In this type of filter, the Use Contact's Value field is not applicable.

Use Contact's Value

Specifies that the filter uses the Field Name value that is associated with the current user.

For example, if you select this check box and you select cost center for Field Name, the users can access product data for their cost centers only. If you apply the filter to all users in the product, the data dynamically filters based on each user cost center. If the cost center changes, the product filters the data for the new cost center automatically.

Note: If you select this check box, the filter limits data based on the Field Name value that is associated with the current user. In this type of filter, the Operator and Value fields are not applicable.

Right Parenthesis

Specifies the last criterion in a group of criteria. You can define groups of criteria to control the logic of the filter.

Note: If you select Right Parenthesis to define the last criterion in a group, select Left Parenthesis for the first criterion in the group.

For example, you can filter for assets with the asset name OE001 or with both the asset family Computer and the asset name Dell. In this example, the group consists of two criteria. The Left Parenthesis is selected for the first criterion, which states that the asset family is Computer. The Right Parenthesis is selected for the second criterion, which states that the asset name is Dell.

Connector

Specifies the connector between a set of two criteria:

- And–Filters the data if the current criterion and the next criterion in the list are valid.
- Or–Filters the data if either the current criterion or the next criterion in the list is valid.

For example, you can filter for assets with an asset family of Computer and an asset name of Dell.

Value

Specifies the field value that you want to filter. If you specify a value, select an Operator in the Operator field. If a Search icon appears next to this field, you can also select a value by clicking the Search icon.

For example, you can filter an asset with an asset name of OE001.

Note: If you specify an Operator and Value, the filter limits data based on a fixed value for the Field Name. In this type of filter, the Use Contact’s Value field is not applicable.

9. Click the Complete Record Edit icon.
10. (Optional) Click Add Fields to define more filter criteria.
11. Click Save after you have completed all filter criteria.

    The filter is defined and applied to users and roles. The data that matches the filter criteria is accessible to filter users.

Example: Filter Asset Data by User Cost Center

As the system administrator, Sam defines a filter that restricts users to the asset data for their own cost centers. To define this filter, Sam makes the following selections:

1. In the Filter Information area, Sam selects Asset in the Object field and (All Families) in the Family field.
2. In the Filter Security area, Sam selects the users who are associated with the filter.
3. In the Filter Criteria area, Sam creates a criterion by performing these steps:
   a. Sam selects Cost Center in the Field Name field.
   b. Sam selects the Use Contact's Value check box.
4. Sam saves the filter.

Verify the Filter

Verify that your filter works to ensure the security of your organizational data.

Follow these steps:

1. Log in to the product as a user who was assigned to the filter.
2. View some of the data that the filter allows for the user.
3. Attempt to view some of the data that the filter does not allow for the user.

   For example, log in as another user who has access to data that is not allowed for the filter user. Copy the URL for a page that displays some data that the filter user cannot access. Paste the URL in the browser of the filter user.

   An error message appears.
4. Attempt to modify some of the data that the filter does not allow for the user.

   For example, identify a text entry field on a page. Enter data that the user cannot access (such as a specific company name that the filter does not allow) and click Save.

   An error message appears.

Example: Verify that the Data Filter Limits Asset Data

Sam created a filter for Asset (All Families) data and assigned the filter to a particular user. With the filter, the user can access only the assets that are in the user cost center. Sam then performs these steps to verify that the filter works:

1. Logs in as the assigned user and validates that assets are available on the Asset Search page.
2. Logs in as a second user with access to assets that are outside of the first user cost center.
3. Views an asset that is outside of the first user cost center and copies the URL of the asset.
4. Logs in as the first user (who was assigned the filter) and pastes the copied asset URL in the browser.

   An error message states that the asset does not exist.

Chapter 7: How to Delete Unused Files from CA APM

This section contains the following topics:

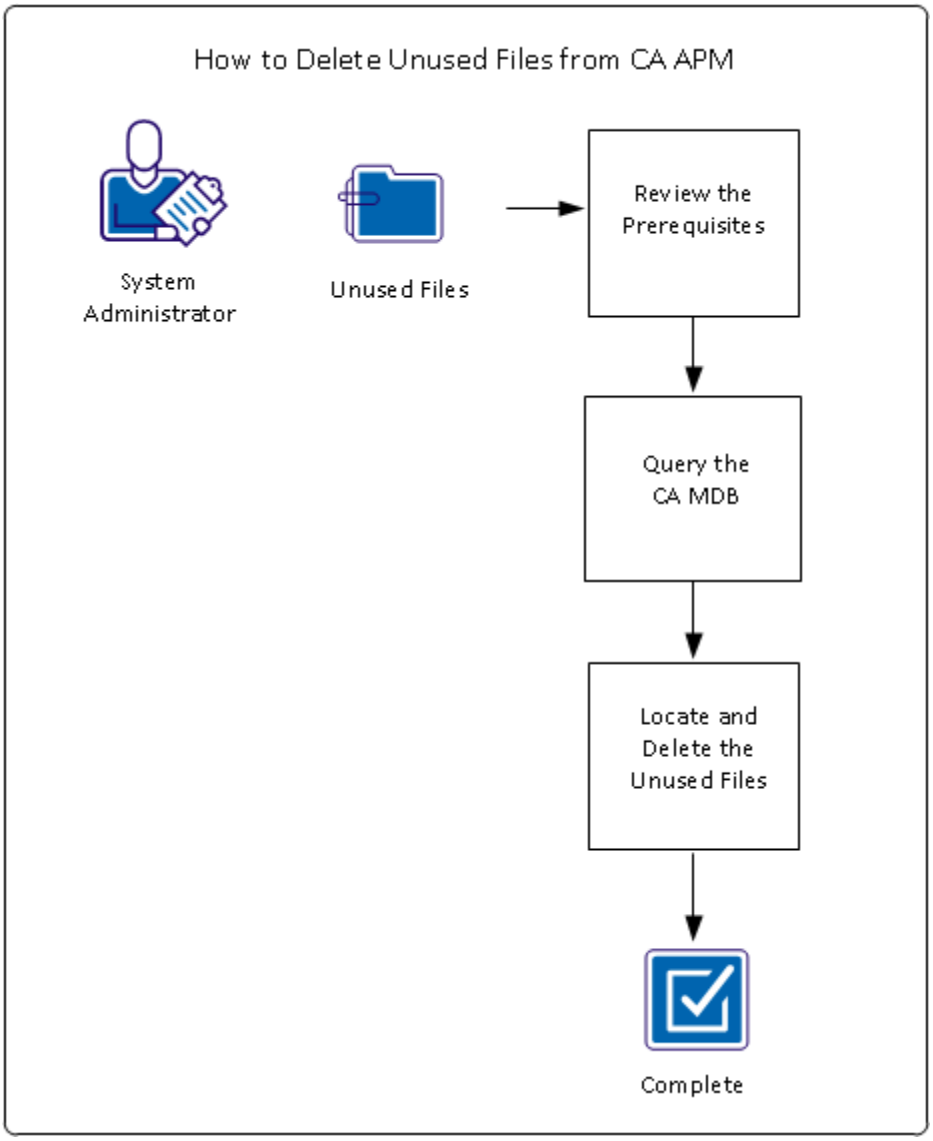
How to Delete Unused Files from CA APM

The files that you use while working with the product are stored on the CA APM application server where the Storage Manager Service is installed. These files include attachment files and Data Importer source data files and legacy map files.

When you delete an attachment, you delete only the reference to the attachment in the object record. If the deleted attachment is a file, the file remains in the file system on the CA APM application server. In similar fashion, when you delete an import that uses a specific data file, you do not delete the data file from the CA APM server.

If a specific attachment file, import data file, or legacy map file is no longer needed, you can delete the file from the CA APM server. Before you delete the file, verify that the file does not have any associations.

The following diagram illustrates how a system administrator deletes unused files from the CA APM application server.



To delete unused files, perform these steps:

1. Review the Prerequisites (see page 163).
2. Query the CA MDB (see page 163).
3. Locate and Delete the Unused Files (see page 163).

Review the Prerequisites

To ensure that you can successfully delete the unused files, identify the names of the unused files that you want to delete.

Query the CA MDB

If a specific attachment file, import data file, or legacy map file is no longer needed, you can delete the file from the CA APM application server. Before you delete the file, verify that the file does not have any associations in CA APM (for example, a file attached to a legal document or an import data file associated with a data import).

Follow these steps:

1. Access the CA MDB that is associated with your CA APM installation.
2. Query the al_file_storage table to search for the file name and the associated tenant if applicable. The following statement is an example query:

   ```
   select COUNT(0) from al_file_storage where attachment_url = 'filename.txt'
   ```

   If no records are returned, no records are associated with the specified file name. You can delete the file.

Locate and Delete the Unused Files

After you verify that the files do not have any associations in CA APM, you can locate and delete the files.

Follow these steps:

1. On the CA APM application server where the Storage Manager Service is installed, navigate to one of the following locations, depending on whether you are using multi-tenancy:

   ```
   [ITAM Root Path]/Storage/Common Store/Attachments
   ```

   ```
   [ITAM Root Path]/Storage/Tenant_Name/Attachments
   ```

   ```
   [ITAM Root Path]/Storage/Common Store/Import
   ```

   ```
   [ITAM Root Path]/Storage/Tenant_Name/Import
   ```

2. Locate and delete the unused files.

Chapter 8: How to Import Data

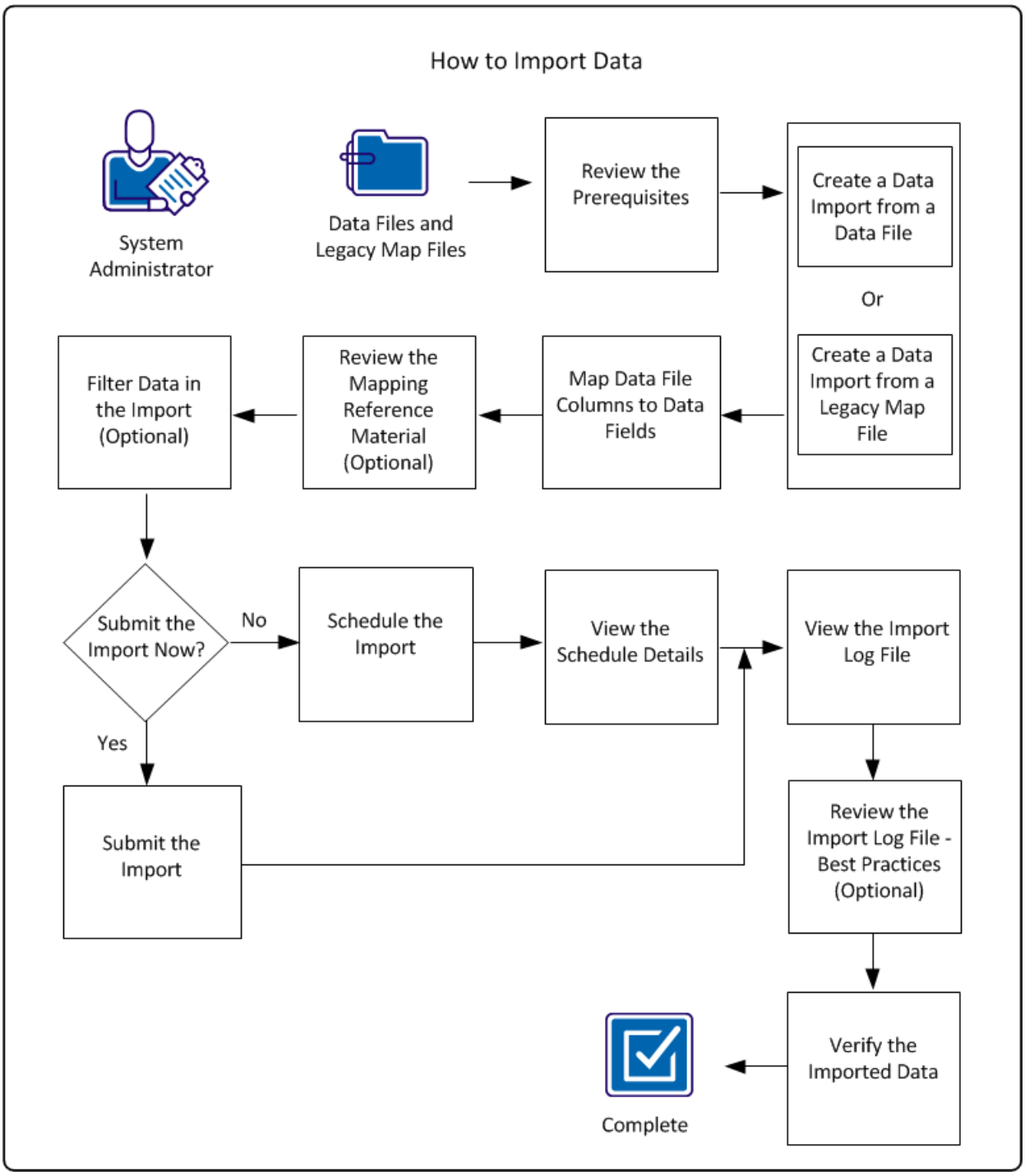
This section contains the following topics:

How to Import Data

When you want to add or update data, import it into CA APM using the Data Importer. The data that you import is inserted, or updates existing data, in the CA MDB.

Important! In this scenario, the system administrator performs the data import. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

The following diagram illustrates how a system administrator imports data.



To import CA APM data, perform these steps:

1. Review the Prerequisites (see page 168).
2. Create a Data Import from a Data File (see page 169) or Create a Data Import from a Legacy Map File (see page 173).
3. Map Data File Columns to Data Fields (see page 174).
4. Review the Mapping Reference Material (see page 176).
   - Primary and Secondary Lookup Combinations (see page 176)
   - Hard-Coded Values (see page 178)
   - Multiple Values for a Single Field (see page 179)
5. Filter Data in the Import (see page 179).
6. Submit the Import (see page 181).
7. Schedule the Import (see page 182).
8. View the Schedule Details (see page 183).
9. View the Import Log File (see page 184).
10. Review the Import Log File Best Practices (see page 184).
11. Verify the Imported Data (see page 185).

Example: Import New Employees

Sam, the CA APM system administrator at Document Management Company, wants to import a group of new employees. The new employees use the product to manage hardware assets. Sam received a comma-separated value (CSV) source data file from Human Resources that contains the employee information. All of the new asset manager employees belong to the IT department and work at the company headquarters. However, the source data file also contains data about some new employees who work at other locations and do not belong to the IT department.

Sam only wants to import the data for the IT employees at headquarters. Using the Data Importer and the source data file, Sam creates a data import to incorporate the new employees into the CA MDB. To ensure that only employees in the IT department at headquarters are imported, Sam creates an exclusion filter. After Sam runs the import, he checks the import statistics and the import log file and user interface to verify that the import was successful.

Review the Prerequisites

To ensure that you can successfully import the data, verify that you have completed the following tasks:

- Prepare a source data file in delimited text format (for example, tab or comma). This file contains the data that you want to import.

  Note: We recommend that you include the main destination object in the name of the source data file. This file naming convention helps you locate your data files when you create your import.

  Note: A value of NULL in your source data file clears the corresponding destination field value. An empty field in your source data file leaves the corresponding destination field value unchanged.

  Important! If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks:

  "Document Management Company, Inc"

- (Optional) Copy your source data files from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

  `[ITAM Root Path]\Storage\Common Store\Import`

  `[ITAM Root Path]\Storage\`*`Tenant_Name`*`\Import`

  Note: If you copy the data file before you create an import, you can then specify the file name when you create the import. If you do not copy the data file first, you can upload the file from your local server when you create the import.

- (Optional) Copy your legacy map files from a previous product release (if you have these files) from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

  `[ITAM Root Path]\Storage\Common Store\Import`

  `[ITAM Root Path]\Storage\`*`Tenant_Name`*`\Import`

Create a Data Import from a Data File

You create a data import using a source data file (delimited text file) that contains the data that you want to import. You select the file, configure the import parameters, and specify the delimiter (for example, a comma or a tab) that separates the data in the file.

You can also create a data import using a legacy map file from a previous product release. For more information, see creating a data import from a legacy map file (see page 173).

Follow these steps:

1. Log in to CA APM as the administrator.

   Important! In this scenario, the system administrator performs the data import. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

2. Click Administration, Data Importer.
3. Click New Import.
4. Enter the required information in the Basic Information area and supply optional information as needed. The following fields require explanation:

   Data File

   Specifies the source data file that you want to import.

   If this file is available on the CA APM application server, search for the data file and select the file. If this file is not available on the application server, upload the file.

   Upload File

   Browse on your local server for a source data file that you want to import or a legacy map file that you want to use to create mappings. This file is uploaded to the CA APM application server.

   Important! The file size is limited by the product environmental settings. For more information, contact your administrator.

Main Destination Object

Specifies the main object for the import.

Asset and Model objects are listed with their corresponding families. You can also specify All Families. Legal Document objects are listed according to legal template. You can also specify All Templates. The objects include all objects that can be imported.

Note: For assets or models that include multiple asset family types or legal documents that include multiple legal templates, use the following selections for this field. Specify the particular family or template for each record in your source data file.

- For an asset, select Asset (All Families).
- For a model, select Model (All Families).
- For a legal document, select Legal Document (All Templates).

Important! Ensure that you select the correct main destination object for your import. You cannot change the main destination object after you save or copy an import.

First Row Has Column Names

Specifies whether the first row in the source data file contains the column names. If the first row does not contain the column names, the names display as generic names, such as Field 1 and Field 2.

Tenant

Specifies the tenant that applies to the import (if you are using multi-tenancy).

You can select a tenant only when multi-tenancy is enabled in CA APM and you are authorized to access different tenants. If you have access to public data and you have multiple tenants, you can select all tenants.

Note: If you specify all tenants, your source data file must have a tenant name column that you map to the Tenant Name field.

Important! If you specify one tenant, verify that all data in your source data file belongs to your selected tenant. If you have data for more than one tenant, data for all tenants is imported into the selected tenant.

Data Delimiter

Specifies the delimiter (for example, comma or tab) that you used in the source data file.

Important! If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks:

"Document Management Company, Inc"

Data File Locale

Specifies the locale for the source data file. This setting determines the date and time format.

5. Enter the required information in the Advanced Settings area and supply optional information as needed. The following fields require explanation:

Maximum Error Threshold (in %)

Defines the number of errors after which the import stops. The threshold is based on the percentage of records processed. We recommend a minimum threshold of 15 percent.

Note: The Data Importer processes the number of records that are specified on Administration, System Configuration, Data Importer (Maximum Batch Record Size field) before calculating if the error threshold has been reached.

Primary Lookup Object Processing Type

Specifies the type of import activity (for example, insert or update).

Create Secondary Lookup Object

Creates new secondary lookup objects during the import process. If this option is not selected and a secondary object does not exist, an error occurs.

Update Secondary Lookup Object

Updates the existing secondary lookup objects during the import process. If a secondary object does not exist, an error occurs.

Error on Secondary Lookup Object Errors

Indicates that the Data Importer does not process a primary object insert or update if the secondary object process fails. If a secondary object insert or update process fails and this check box is selected, the insert or update for the primary object also fails. If this check box is not selected, the primary object is created or updated (as long as the object is not dependent on the secondary object). However, the secondary object value is not created or changed. In both situations, the secondary object error is logged in the import log file.

Example: You import a location and the location has a country. If the import fails while trying to update the country object and this check box is selected, the location record is not created. If this check box is not selected, the location record is created, and the country information is not updated.

Normalization Behavior

Specifies whether to normalize the data or write an error message in the log file without normalizing the data.

Note: This field appears only if you have defined normalization rules.

Error on Normalization

Writes an error message to the Data Importer log file when data that can be normalized is found in the data that you are importing. The data involved is not imported. The log file error message includes the details about the data.

For example, your data includes the company name Microsoft. The company normalization rules that you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when importing your data, the object with the company name Microsoft is not imported and an error message is written to the log file.

Apply Normalization without Error

Uses the normalization rules to normalize the data that you are importing. If data that can be normalized is found, the data is normalized and imported. No error message about the data is written to the log file.

For example, your data includes the company name Microsoft. The company normalization rules you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when importing your data, the object with company name Microsoft is normalized. In this example, the company name is changed to Microsoft Corporation and the associated object is imported.

6. Click Save.

The import is saved. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input.

Example: Create a Data Import of New Employees from a Data File

Sam, the CA APM system administrator, performs the following actions to create the data import:

1. Navigates to Administration, Data Importer and clicks New Import.
2. Enters New Employees.csv in the Data File field.

   This CSV file is the source data file that Sam received from Human Resources with the new employee information.
3. Selects Contact for the Main Destination Object and comma for Data Delimiter.
4. Selects Insert or Update in the Primary Lookup Object Processing Type field and clicks Save.

Create a Data Import from a Legacy Map File

You can create a data import using a legacy map file from a previous CA APM release. The map file defines the corresponding data file and the import parameter settings.

Note: We recommend that you copy your legacy map files and corresponding data files to the CA APM application server before you create the data imports. However, if necessary, you can use the optional steps to upload a legacy map file.

You can also create a data import using a data file only. For more information, see creating a data import from a data file (see page 169).

Follow these steps:

1. Click Administration, Data Importer, New Import.
2. Click Search and Load Map to select a legacy map file that is already available on the CA APM application server.

   Important! The corresponding data file must also be available on the CA APM application server.

   If the legacy map file is not available on the CA APM application server, upload the file using the Upload File field.

3. (Optional) Upload a legacy map file that is not available on the CA APM application server using the following steps:

   a. In the Upload File field, browse on your local server and select a legacy map file.

      The legacy map file is uploaded and is displayed in the Upload File field.

   b. Click Search and Load Map and select the legacy map file that you uploaded.

      The legacy map file is displayed in the Legacy Map File field.

      The Basic Information is loaded.

   Note: If you receive a warning about the source data file, upload the data file using the Upload File field.

4. Specify the Advanced Settings and click Save.

   The Exclusion Filter and Mapping data mapping are loaded. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input. The Mapping and Exclusion Filter areas display the data from the legacy map file.

   Note: For information about specifying the Advanced Settings, see creating a data import from a data file (see page 169).

Map Data File Columns to Data Fields

You can map the columns in your source data file to fields in CA APM. You perform column mapping to specify where the source data is imported. You can select most objects and associated fields as destination fields during column mapping.

Note: If you created your data import from a legacy map file, the column mapping exists. If you want to change the values, you can edit the existing mapping rules. You can also add or remove mapping rules and filters.

When you log in, the user role that your administrator assigned to you determines the objects and fields that you can see and use. If your role specifies that you do not have permissions for an object field, the field is not available for a mapping. You can only create a mapping and import data for the objects and fields for which you have permissions.

Note: We recommend that, before you map data, you review the CA APM user interface to determine the required information for a mapping. For example, review the Asset page to see that the asset name, asset family, model, and class are required. Because a model is required to create an asset, you review the Model page to see that the model name and asset family are required. By reviewing the user interface before you create a mapping, you ensure that you have all required information to create a mapping.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Mapping area for a selected import, click New or click Load Source Fields.

   - New allows you to select the source fields individually from the source data file.
   - Load Source Fields adds all source fields from the source data file.

   Note: If you have existing mappings, Load Source Fields allows you to replace those mappings with the source fields in the source data file. This option also allows you to add the source fields from the source data file that you do not already have in your mappings.

   a. If you clicked Load Source Fields, click the Edit Record icon next to a field.

2. Click the Select icon next to Source Field (if this field is empty), select a column from your data source, and click OK.

   If this field already contains a source field (because you loaded all source fields), you can skip this step.

   Note: The percent signs that appear before and after the column names identify the names as column headers in your source data file. You can also specify a hard-coded value in the Source Field that you want to apply to all records in your source data file. You can then map the hard-coded value to a Destination Field. The hard-coded values do not display with percent signs so that they can be distinguished from the source data file column names. For more information, see hard-coded values (see page 178).

3. Click the Select icon next to Destination Field, select a Destination Field for the selected Source Field, and click OK.

   The destination fields that appear are based on your selected main destination object.

   Note: The destination fields display in hierarchical order. For example, the fields that are listed under Asset Type Hierarchy are Asset Family, Class, and Subclass. The order of the fields in the list represents the field hierarchy. Follow the field hierarchy when you specify mapping rules. For example, for Asset Type Hierarchy, specify a rule for Class before you specify Subclass.

4. Select the Primary Lookup and Secondary Lookup check boxes as required.

   a. Select a Primary Lookup check box for each destination field that you want to use to find the primary object. Use the following guidelines when selecting this check box:

      - Select at least one Primary Lookup check box in the column mapping for an import.
      - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

b. Select a Secondary Lookup check box for each destination field that you want to use to find the secondary objects. Use the following guidelines when selecting this check box:

- Do not select this check box if the destination field is not one of your lookup fields for the secondary object.
- Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

5. Click the Complete Record Edit icon.
6. Click New again, or click the Edit Record icon next to another source field, to specify more mapping rules.

   Note: To delete a specific mapping rule from the list of mapped columns, click the Deletion icon next to the mapping rule. The column mapping rule is removed from the list.
7. Click Save.

   Your column mapping is saved.

Example: Map Data File Columns to Data Fields

Sam performs the following steps to map the data file columns in the source data file to the CA APM data fields:

1. Clicks New in the Mapping area of the Import Details page.
2. Selects %Login ID% in the Source Field by clicking the Select icon next to Source Field and selecting this item from the dialog.

   The items that are listed in the dialog are the columns from the source data file.
3. Selects User ID in the Destination Field by clicking the Select icon next to Destination Field and selecting this object from the dialog.
4. Selects the Primary Lookup check box.
5. Continues to map the remaining columns in the source data file with CA APM data fields and clicks Save when finished.

Review the Mapping Reference Material

Reference the following information when setting up the column mapping for importing or deleting data.

Primary and Secondary Lookup Combinations

The fields that you select as the primary and secondary lookup in your column mapping are used to search for data in the product database.

Simple mapping

In simple mapping, you specify only the primary lookup. For example, you are importing or deleting a set of company records from a text file into the product database. You specify the Company Name as the primary lookup. If a company with a particular name does not exist in the database when you are importing data, a record is created for the company. The following table shows an example of the lookup for a simple mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No

Reference field mapping

In reference field mapping, you specify primary and secondary lookup values. To search for a unique object, specify more than one primary lookup. For example, to search for a company, you can specify Company Name, Parent Company, and Company Type as primary lookup values. In this example, the Data Importer searches for a company with the specified name, the specified parent company, and of the specified company type. If the object does not exist and you are importing data, the record is created (depending on the insert or update option you selected in Advanced Settings). The following table shows an example of the lookup for reference field mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No
%Parent Company%	Company.Parent Company.Company Name	Yes	Yes
%Company Type%	Company.Company Type.Value	Yes	Yes

This mapping has both the Primary Lookup and the Secondary Lookup check boxes selected for Parent Company and Company Type. The Data Importer uses the Company Name to look up the parent company and uses the Parent Company to look up the company name.

Secondary object mapping

If a mapping rule maps to a secondary object property, the primary lookup values establish a relationship between a secondary object and the reference fields. The following table shows examples of the lookup for a secondary object mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Comment%	Legal Document.Legal Party.Comment	No	Yes
%Legal Document ID%	Legal Document.Document Identifier	Yes	No
%Company Name%	Legal Document.Legal Party.Legal Party.Company Name	Yes	Yes
%Legal Template%	Legal Document.Legal Template.Template	Yes	Yes

In the first mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. Comment is a property of Legal Party.

In the third mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. In addition, Legal Party has a reference field in the Company table. The Secondary Lookup check box indicates that the Company Name is used to look up the Company object. The Primary Lookup check box indicates that the Company object is used to look up the Legal Party object.

Hard-Coded Values

In the column mapping, the percent signs that appear before and after column names identify the names as column headers in your source data file. You can also specify a hard-coded value in the Source Field that you want to apply to all records in your source data file. You can then map the hard-coded value to a Destination Field. The hard-coded values do not display with percent signs to distinguish these values from the source data file column names.

1. Source data file column header
2. Hard-coded value

You can define a hard-coded value in the Source Field to expand your source data and to ensure that you include all required fields. Hard-coded values typically do not begin and end with a percent sign (%). If you have hard-coded values with percent signs, the values cannot match the field names in your source data file.

Example: Use hard-coded values for asset family

In this example, the assets in your source data file do not contain asset family, which is required when creating an asset. You can add a hard-coded value to your mapping. If all of your assets are hardware, you can enter Hardware in the Source Field. You can map this value to the Asset Family field. If your assets belong to different families, add a column to your source data file with the corresponding asset families before importing or deleting data.

The following information illustrates the difference between values from your source data file and values that are added through hard-coded values:

- You have an Asset Family column in your source data file. The selection in the Source Field is %asset family%.
- You do not have an Asset Family column in your source data file. However, all of your assets are hardware assets. You specify a hard-coded value of Hardware in the Source Field.

  Note: You can also use the Main Destination Object to specify that all records in your source data file belong to a particular family or template. For example, the Asset (Hardware) selection for Main Destination Object specifies that all source records belong to the hardware asset family.

Multiple Values for a Single Field

You can add a mapping with multiple Source Field values that are mapped to a single Destination Field.

Example: Use multiple values for a single field

Your source data file has two columns with the names Manufacturer and Catalog Name. Combine these columns by selecting both in the Source Field. In this example, the Source Field selection is %Manufacturer% %Catalog Name%.

You can also enter multiple hard-coded values in the Source Field (for example, Document Management Company %model name% IT Department).

Filter Data in the Import

You can identify a subset of records in your source data file that you want to exclude from the import. The Data Importer exclusion filter allows you to filter a part of your data source using exclusion filter rules.

Example: Define an exclusion filter to process returned assets

A CSV file that you receive from your hardware vendor includes assets that were ordered and returned to the vendor. You want to process only the returned assets, so you want to import data to update those records only. You define an exclusion filter to exclude records that do not have a status of Returned.

Follow these steps:

1. On the Administration tab, Data Importer page, Exclusion Filter area for a selected import, select the Filter Type.

   And

   Excludes a record from the source data file only if all the rules that you specify are valid for the record.

   Or

   Excludes a record from the source data file if any of the rules that you specify is valid for the record.

2. Click New.
3. Click the Select icon next to Source Field, select a column from your source data file, and click OK.

   Note: The percent signs before and after the column names identify the names as columns from your source data file.

4. Select the Operator.

   Note: To specify "not equal to", select the "<>" operator.

5. Enter a Filter Value for the rule.

   Note: You can use special characters and wildcards in the filter value. The rules can process text, numeric, and date fields.

6. Click the Complete Record Edit icon.
7. (Optional) Click New and specify more exclusion filter rules.
8. Click Save.

   The exclusion filter rules are saved and are applied when the import processes.

Example: Create an Exclusion Filter

Sam performs the following steps to create an exclusion filter. The filter eliminates non-IT employees and employees who do not work at the company headquarters from the data import.

1. Selects And for the Filter Type and clicks New in the Exclusion Filter area of the Import Details page.
2. Selects %Department% for the Source Field.
3. Selects <> for the Operator.
4. Enters IT for the Filter Value.
5. Clicks the Complete Record Edit icon and clicks New.
6. Selects %Location% for the Source Field.
7. Selects <> for the Operator.
8. Enters Headquarters for the Filter Value.
9. Clicks the Complete Record Edit icon and clicks Save.

Submit the Import

To start an import immediately, click Submit in the Schedule area of the page. The data source records from the data file for the selected import are processed.

Note: You can specify a data file other than the default (from the Basic Information) if you want to use a different file.

You can also schedule the import for a particular day and time. For more information, see schedule the import (see page 182).

To view the import jobs for your current selected import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs on the left side of the page. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

Schedule the Import

You can schedule an import for a specific time and you can specify the interval for the import (for example, daily or weekly). You can schedule multiple imports to process simultaneously.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Schedule area for a selected import, select the Is Scheduled check box.
2. Provide the information for the schedule. The following fields require explanation:

   Run Time

   Specifies the time of the day, in 24-hour format, to process the import. When you schedule imports, use the local time zone on the CA APM application server.

   Interval Day

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

   Data File

   Specifies a data file name other than the default (from the Basic Information) if you want to use a different file.

   If this file is available on the application server, you can search and select the file. If this file is not available on the application server, you can locate and upload the file.

   Upload Data File

   Browse for the source data file that you want to import. This file is uploaded to the application server.

   First Run Date

   Specifies the date when the first import starts to process.

   Interval Type

   Specifies the type of interval for the import (for example, Day, Month, Quarter, Week, or Year).

Interval

Specifies how often the import processes. This interval is based on the specified Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the import processes every two weeks.

Last Day of Interval

Specifies that the import processes on the last day of the selected Interval Type. If you select this check box, any previous value that you added to the Interval Day field is removed, and the Interval Day field is disabled.

3. Click Submit.

   The data import is scheduled for the specified date and time.

Examples: Using the Schedule Settings

The following examples illustrate the use of the schedule settings.

- Select Day for Interval Type and 2 for Interval. The import processes every other day.
- Select Week for Interval Type, 1 for Interval Day, and 3 for Interval. The import processes every three weeks on the first day of the week (Sunday).
- Select Month for Interval Type, 15 for Interval Day, and 2 for Interval. The import processes every two months on the 15th day of the month.
- Select Quarter for Interval Type and select Last Day of Interval. The import processes every quarter (every three months) on the last day of the last month in the quarter.
- Select Year for Interval Type, 1 for Interval Day, and 1 for Interval. The import processes on January 1 of every year.

To view the import jobs for your current selected import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs on the left side of the page. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

View the Schedule Details

You can view the schedule details for a scheduled import job that you created.

First, open the list of import jobs.

- To view the scheduled import jobs for your currently selected import, click Associated Jobs on the left side of the page, select the Scheduled check box, and click Go.
- To view all import jobs for all imports, click Import Jobs on the left side of the page, select the Scheduled check box, and click Go.

In the list of import jobs that appears, click Schedule Details for a selected import.

View the Import Log Files

You can view the Data Importer log files to see the details of all CA-provided and user-defined imports that have completed. The Data Importer creates a log file for each import that you run, including imports that were submitted immediately or scheduled for a future time. All import activities are saved in the log files.

To view the log files, first open the list of import jobs.

- To view the import jobs for your current selected import, click Associated Jobs on the left side of the page.
- To view all import jobs for all imports, click Import Jobs.

In the list of import jobs, click View Logs for a selected import. If more than one log file is available (for example, for a scheduled import that has completed a few times already), all files are listed with their corresponding creation dates.

You can view any available LDAP Import Sync log file. If you click Start LDAP Data Import and Sync on the LDAP Data Import and Sync page (Administration, User/Role Management), an import job ID is displayed. Use this job ID to locate the job in the Data Importer list of import jobs. Then click View Logs for that job.

Note: You can also locate and view the import log files in the following location on the CA APM application server:

```
[ITAM Root Path]\Storage\Common Store\Import\Logs
```

Review the Import Log File - Best Practices

The Data Importer log file contains information and error messages regarding the processing of import jobs. To help you understand the results of your import and to troubleshoot any errors, use the information in this log file. This section contains some recommended best practices for working with the Data Importer log file.

Match the row number in the data file with the error message in the log file.

A log file error message identifies the corresponding row number from your data file. You can also find the data file row number in the row above or below the error message in the log file.

Sometimes the error message in the log file does not show the data file row number. In this situation, the actual data file values are shown immediately after the error message in the log file.

Count the number of error messages in your log file.

1. Search for the following phrases in your log file to find the error messages in the file. These phrases are included with the error messages.

   ```
   Web Service threw exception
   ```

   ```
   Error at record
   ```

2. After you find a type of error message, search for that error in the log file and count the number of occurrences.
3. Identify and search for more error types that appear in your log file and count the number of occurrences.
4. Compare the count of all errors in your log file with the statistics that the Data Importer generated for the associated import. To view these statistics, click Status Message on the Associated Jobs list or Import Jobs list. This comparison helps you account for all relevant errors and identify error messages that are not valid and can be ignored.

Verify the Imported Data

You verify that your data import succeeded by viewing your data in CA APM and by reviewing the Data Importer statistics.

- **Review the Data Importer Statistics.** To review the statistics for your current selected import, click Associated Jobs on the left side of the page. In the list of import jobs that appears, click Status Message for your import.

  You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

- **View the Imported Data in CA APM.** To view the imported data, navigate to the tab and subtab, if necessary, for the object that you imported (for example, asset, company, or contact). Search for the objects that you imported and verify that the objects are available.

Example: Verify the Data Import of New Employees

After Sam runs the import, he performs the following steps to verify the data import of new employees:

1. Checks the import statistics.
   - Clicks Associated Jobs or Import Jobs on the left side of the Data Importer page.
   - Clicks Status Message for the import and reviews the statistics.
2. Views the import log file and the user interface.
   - Clicks View Logs in the list of import jobs and reviews the contents of the log file.
   - Navigates to Directory, Contact on the CA APM user interface. Searches for the new employees. Verifies that the non-IT employees and employees who do not work at company headquarters are not available.

Chapter 9: How to Delete Data with the Data Importer

This section contains the following topics:

How to Delete Data with the Data Importer

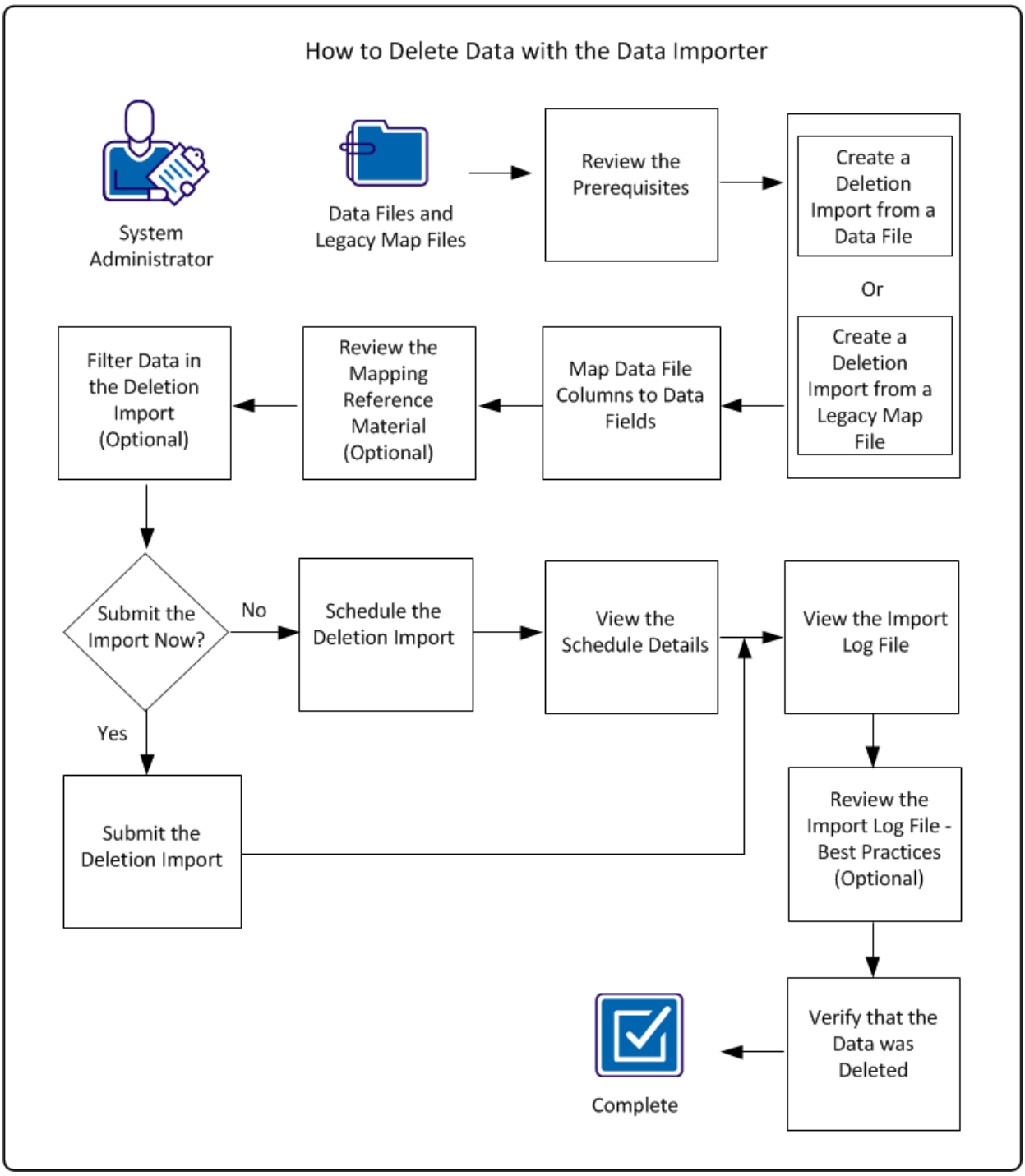
When data is no longer valid for your implementation, delete the data from CA APM using the Data Importer. In most situations, however, it is considered good IT asset management practice to keep the data in the repository with a status of inactive. This method allows you to access the data for historical and audit purposes. However, in some cases, the data was created by mistake. In these cases, you want to delete the data.

Important! In this scenario, the system administrator performs the data deletion. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

You can delete primary objects and can remove the relationships to their secondary objects. For example, you delete an asset (primary object) and you remove its relationship to a legal document (secondary object).

When you delete a primary object and its relationship to a secondary object, the secondary object is not deleted. The primary object is deleted, and the relationship between the primary and secondary object is removed. For example, if you delete an asset and its associated legal document relationship, the asset is deleted but the legal document is not deleted. Only the relationship between the asset and the legal document is removed.

The following diagram illustrates how a system administrator deletes data.



To delete CA APM data, perform these steps:

1. Review the Prerequisites. (see page 190)
2. Create a Deletion Import from a Data File (see page 191) or Create a Deletion Import from a Legacy Map File (see page 195).
3. Map Data File Columns to Data Fields. (see page 196)
4. Review the Mapping Reference Material. (see page 176)
   - Primary and Secondary Lookup Combinations (see page 176)
   - Hard-Coded Values (see page 178)
   - Multiple Values for a Single Field (see page 179)
5. Filter Data in the Deletion Import (see page 201).
6. Submit the Deletion Import (see page 202) or Schedule the Deletion Import (see page 203).
7. View the Schedule Details (see page 183).
8. View the Import Log File. (see page 184)
9. Review the Import Log File - Best Practices (see page 184).
10. Verify that the Data was Deleted (see page 206).

Example: Delete Laptops

Miriam, the CA APM system administrator at Document Management Company, wants to delete several laptops that have been retired and recycled. Miriam also wants to delete the associations with legal documents that were made for these laptops. Miriam has a data file that identifies the laptop names, the manufacturers, and the model names. Using the Data Importer and the source data file, Miriam creates a deletion import. After Miriam runs the import, she views the import statistics, import log file, and user interface to verify the deletions.

Review the Prerequisites

To ensure that you can successfully delete the data, verify that you have completed the following tasks:

- Prepare a source data file in delimited text format (for example, tab or comma) containing the data that you want to delete.

  Note: We recommend that you include the main destination object in the name of the source data file. This file naming convention helps you locate your data files when you create your import.

  Note: A value of NULL in your source data file clears the corresponding destination field value. An empty field in your source data file leaves the corresponding destination field value unchanged.

  Important! If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks:

  "Document Management Company, Inc"

- (Optional) Copy your source data files from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

  `[ITAM Root Path]\Storage\Common Store\Import`

  `[ITAM Root Path]\Storage\Tenant_Name\Import`

  Note: If you copy the data file before you create an import, you can then specify the file name when you create the import. If you do not copy the data file first, you can upload the file from your local server when you create the import.

- (Optional) Copy your legacy map files from a previous product release (if you have these files) from your local server to one of the following locations. You can access these locations on the CA APM application server where the Storage Manager Service is installed. The location depends on whether you are using multi-tenancy.

  `[ITAM Root Path]\Storage\Common Store\Import`

  `[ITAM Root Path]\Storage\Tenant_Name\Import`

Create a Deletion Import from a Data File

You can delete data using a source data file (delimited text file) that contains the data that you want to delete. You select the file, configure the import parameters, and specify the delimiter (for example, a comma) that separates the data in the file.

You can also create a deletion import using a legacy map file from a previous product release. For more information, see creating a deletion import from a legacy map file (see page 195).

Follow these steps:

1. Log in to CA APM as the administrator.

   Important! In this scenario, the system administrator performs the deletion import. However, the administrator can grant Data Importer User Access or Data Importer Admin Access to any CA APM user role. User access allows users to create imports, modify or delete their own imports, and view any import that was created by another user. Admin access allows users to create imports and modify or delete any import that was created by any user.

2. Click Administration, Data Importer.
3. Click New Import.
4. Enter the required information in the Basic Information area and supply optional information as needed. The following fields require explanation:

   Data File

   Specifies the source data file.

   If this file is available on the CA APM application server, search for the data file and select the file. If this file is not available on the application server, upload the file.

   Upload File

   Browse on your local server for a source data file or a legacy map file that you want to use to create mappings. This file is uploaded to the CA APM application server.

   Important! The file size is limited by the product environmental settings. For more information, contact your administrator.

Main Destination Object

Specifies the main object for the deletion import.

Asset and Model objects are listed with their corresponding families. You can also specify All Families. Legal Document objects are listed according to legal template. You can also specify All Templates. The objects include all objects that can be imported or deleted.

Note: For assets or models that include multiple asset family types or legal documents that include multiple legal templates, use the following selections for this field. Specify the particular family or template for each record in your source data file.

- For an asset, select Asset (All Families).
- For a model, select Model (All Families).
- For a legal document, select Legal Document (All Templates).

Important! Ensure that you select the correct main destination object. You cannot change the main destination object after you save or copy an import.

First Row Has Column Names

Specifies whether the first row in the source data file contains the column names. If the first row does not contain the column names, the names display as generic names, such as Field 1 and Field 2.

Tenant

Specifies the tenant that applies to the import (if you are using multi-tenancy).

You can select a tenant only when multi-tenancy is enabled in CA APM and you are authorized to access different tenants. If you have access to public data and you have multiple tenants, you can select all tenants.

If you specify all tenants, your source data file must have a tenant name column that you map to the Tenant Name field.

Note: If you specify one tenant, verify that all data in your source data file belongs to your selected tenant. If you have data for more than one tenant, data for all tenants is applied to the selected tenant.

Data Delimiter

Specifies the delimiter (for example, comma or tab) that you used in the source data file.

Important! If a data value in your source data file contains the selected delimiter, you must use double quotation marks around the data value. For example, you select a comma as the delimiter to import companies. You want to include the data value Document Management Company, Inc. in your source data file. Specify this data value with double quotation marks:

"Document Management Company, Inc"

Data File Locale

Specifies the locale for the source data file. This setting determines the date and time format.

5. Enter the required information in the Advanced Settings area and supply optional information as needed.

   The following fields require explanation:

   Maximum Error Threshold (in %)

   Defines the number of errors after which the import stops. The threshold is based on the percentage of records processed. We recommend a minimum threshold of 15 percent.

   Note: The Data Importer processes the number of records that are specified on Administration, System Configuration, Data Importer (Maximum Batch Record Size field) before calculating if the error threshold has been reached.

   Primary Lookup Object Processing Type

   Specifies the type of import activity. Select one of the following options:

   Delete Primary Objects and Associated Relationships

   Select this option to delete primary objects and the relationships to their associated secondary objects. For example, you delete a company (primary object) and you remove the relationship to an associated asset allocation (secondary object).

   When you select this option, verify that your mapping rules specify the primary objects only. Do not include any mapping rules for secondary objects.

   Note: The secondary object that is associated with a primary object is not deleted. The relationship between the primary object and the secondary object is removed. For example, you have a primary object Company1 with an associated acquired company Company2 (secondary object). When you delete Company1, the relationship to Company2 is removed. The secondary object Company2 is not deleted.

Delete Relationships Only

Select this option to remove the relationships between secondary objects and their primary objects. When you select this option, verify that your mapping rules specify the primary and secondary objects only. You include a mapping rule for a secondary object; however, do not select the Primary Lookup check box for this rule.

Note: A secondary object that is associated with a primary object is not deleted. The relationship between the primary and secondary object is removed.

Normalization Behavior

Specifies whether to normalize the data or write an error message in the log file without normalizing the data.

Note: This field appears only if you have defined normalization rules.

Error on Normalization

Writes an error message to the Data Importer log file when data that can be normalized is found in the data that you are deleting. The data involved is not deleted. The log file error message includes the details about the data.

For example, your data includes the company name Microsoft. The company normalization rules that you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when deleting your data, the object with the company name Microsoft is not deleted and an error message is written to the log file.

Apply Normalization without Error

Uses the normalization rules to normalize the data that you are deleting. If data that can be normalized is found, the data is normalized and deleted. No error message about the data is written to the log file.

For example, your data includes the company name Microsoft. The company normalization rules you created identify Microsoft as a collected (nonauthoritative) value and specify Microsoft Corporation as the normalized (authoritative) value. If you select this option when deleting your data, the object with company name Microsoft is normalized. In this example, the company name is changed to Microsoft Corporation and the associated object is deleted.

6. Click Save.

   The deletion import is saved. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input.

Example: Create a Deletion Import from a Data File

Miriam, the CA APM system administrator, performs the following actions to create the deletion import:

1. Navigates to Administration, Data Importer and clicks New Import.
2. Enters Hardware Deletions.csv in the Data File field.

   This CSV file is the source data file that contains the laptop deletions.
3. Selects Asset (Hardware) for the Main Destination Object and comma for the Data Delimiter.
4. Selects Delete Primary Objects and Associated Relationships in the Primary Lookup Object Processing Type field and clicks Save.

Create a Deletion Import from a Legacy Map File

You can create a deletion import using a legacy map file from a previous CA APM release. The map file defines the corresponding data file and the import parameter settings.

Note: We recommend that you copy your legacy map files and corresponding data files to the CA APM application server before you create the deletion imports. However, if necessary, you can use the optional steps to upload a legacy map file.

You can also create a deletion import using a data file only. For more information, see creating a deletion import from a data file (see page 191).

Follow these steps:

1. Click Administration, Data Importer, New Import.
2. Click Search and Load Map to select a legacy map file that is already available on the CA APM application server.

   Important! The corresponding data file must also be available on the CA APM application server.

   If the legacy map file is not available on the CA APM application server, upload the file using the Upload File field.

3. (Optional) Upload a legacy map file that is not available on the CA APM application server using the following steps:

   a. In the Upload File field, browse on your local server and select a legacy map file.

      The legacy map file is uploaded and is displayed in the Upload File field.

   b. Click Search and Load Map and select the legacy map file that you uploaded.

      The legacy map file is displayed in the Legacy Map File field.

      The Basic Information is loaded.

   Note: If you receive a warning about the source data file, upload the data file using the Upload File field.

4. Specify the Advanced Settings and click Save.

   The Exclusion Filter and Mapping data mapping are loaded. The Mapping, Exclusion Filter, and Schedule areas of the page are now available for your input. The Mapping and Exclusion Filter areas display the data from the legacy map file.

   Note: For information about specifying the Advanced Settings, see creating a deletion import from a data file (see page 191).

Map Data File Columns to Data Fields

You can map the columns in your source data file to product fields. You perform column mapping to specify which data is deleted. You can select most objects and associated fields as destination fields during column mapping.

Note: If you created your deletion import from a legacy map file, the column mapping exists. You can edit the existing mapping rules if you want to change the values. You can also add new mapping rules.

When you log in, the user role that your administrator assigned to you determines the objects and fields that you can see and use. If your role specifies that you do not have permissions for an object field, the field is not available for a mapping. You can only create a mapping and import or delete data for the objects and fields for which you have permissions.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Mapping area for a selected deletion import, click New or click Load Source Fields.

   - New allows you to select the source fields individually from the source data file.
   - Load Source Fields adds all source fields from the source data file.

   Note: If you have existing mappings, Load Source Fields allows you to replace those mappings with the source fields in the source data file. This option also allows you to add the source fields from the source data file that you do not already have in your mappings.

   a. If you clicked Load Source Fields, click the Edit Record icon next to a field.

2. Click the Select icon next to Source Field (if this field is empty), select a column from your data source, and click OK.

   If this field already contains a source field (because you loaded all source fields), you can skip this step.

3. Click the Select icon next to Destination Field, select a Destination Field for the selected Source Field, and click OK.

   The destination fields that appear are based on your selected main destination object.

   Note: The destination fields display in hierarchical order. For example, the fields that are listed under Asset Type Hierarchy are Asset Family, Class, and Subclass. The order of the fields represents the field hierarchy. Follow the field hierarchy when you specify mapping rules. For example, for Asset Type Hierarchy, specify a rule for Class before you specify Subclass.

4. Select the Primary Lookup and Secondary Lookup check boxes as required.

   a. Select a Primary Lookup check box for each destination field that you want to use to find the primary object. Use the following guidelines when selecting this check box:

      - Select at least one Primary Lookup check box in the column mapping for an import.
      - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

   b. Select a Secondary Lookup check box for each destination field that you want to use to find the secondary object. Use the following guidelines when selecting this check box:

      - Do not select this check box if the destination field is not one of your lookup fields for the secondary object.
      - Do not select this check box if the Destination Field is Note Text (under the Note object). The database data type for the Note Text field does not allow it to function as a lookup field.

5. Click the Complete Record Edit icon.
6. (Optional) Click New again, or click the Edit Record icon next to another source field, to specify more mapping rules.

   Note: To delete a specific mapping rule from the list of mapped columns, click the Delete icon next to the mapping rule. The column mapping rule is removed from the list.
7. Click Save.

   Your column mapping is saved.

Example: Map Data File Columns to Data Fields

Miriam performs the following steps to map the columns in the source data file to the CA APM data fields:

1. Clicks New in the Mapping area of the Import Details page.
2. Selects %Hardware Name% in the Source Field by clicking the Select icon next to Source Field and selecting this item from the dialog.

   The items that are listed in the dialog are the columns from the source data file.
3. Selects Asset Name in the Destination Field by clicking the Select icon next to Destination Field and selecting this object from the dialog.
4. Selects the Primary Lookup check box.
5. Clicks the Complete Record Edit icon and clicks Save.

Review the Mapping Reference Material

Reference the following information when setting up the column mapping for importing or deleting data.

Primary and Secondary Lookup Combinations

The fields that you select as the primary and secondary lookup in your column mapping are used to search for data in the product database.

Simple mapping

In simple mapping, you specify only the primary lookup. For example, you are importing or deleting a set of company records from a text file into the product database. You specify the Company Name as the primary lookup. If a company with a particular name does not exist in the database when you are importing data, a record is created for the company. The following table shows an example of the lookup for a simple mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No

Reference field mapping

In reference field mapping, you specify primary and secondary lookup values. To search for a unique object, specify more than one primary lookup. For example, to search for a company, you can specify Company Name, Parent Company, and Company Type as primary lookup values. In this example, the Data Importer searches for a company with the specified name, the specified parent company, and of the specified company type. If the object does not exist and you are importing data, the record is created (depending on the insert or update option you selected in Advanced Settings). The following table shows an example of the lookup for reference field mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Company Name%	Company.Company Name	Yes	No
%Parent Company%	Company.Parent Company.Company Name	Yes	Yes
%Company Type%	Company.Company Type.Value	Yes	Yes

This mapping has both the Primary Lookup and the Secondary Lookup check boxes selected for Parent Company and Company Type. The Data Importer uses the Company Name to look up the parent company and uses the Parent Company to look up the company name.

Secondary object mapping

If a mapping rule maps to a secondary object property, the primary lookup values establish a relationship between a secondary object and the reference fields. The following table shows examples of the lookup for a secondary object mapping.

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Comment%	Legal Document.Legal Party.Comment	No	Yes
%Legal Document ID%	Legal Document.Document Identifier	Yes	No
%Company Name%	Legal Document.Legal Party.Legal Party.Company Name	Yes	Yes

Source Field	Destination Field	Primary Lookup	Secondary Lookup
%Legal Template%	Legal Document.Legal Template.Template	Yes	Yes

In the first mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. Comment is a property of Legal Party.

In the third mapping rule, Legal Document is the primary object, and Legal Party is the secondary object. In addition, Legal Party has a reference field in the Company table. The Secondary Lookup check box indicates that the Company Name is used to look up the Company object. The Primary Lookup check box indicates that the Company object is used to look up the Legal Party object.

Hard-Coded Values

In the column mapping, the percent signs that appear before and after column names identify the names as column headers in your source data file. You can also specify a hard-coded value in the Source Field that you want to apply to all records in your source data file. You can then map the hard-coded value to a Destination Field. The hard-coded values do not display with percent signs to distinguish these values from the source data file column names.

1. Source data file column header
2. Hard-coded value

You can define a hard-coded value in the Source Field to expand your source data and to ensure that you include all required fields. Hard-coded values typically do not begin and end with a percent sign (%). If you have hard-coded values with percent signs, the values cannot match the field names in your source data file.

Example: Use hard-coded values for asset family

In this example, the assets in your source data file do not contain asset family, which is required when creating an asset. You can add a hard-coded value to your mapping. If all of your assets are hardware, you can enter Hardware in the Source Field. You can map this value to the Asset Family field. If your assets belong to different families, add a column to your source data file with the corresponding asset families before importing or deleting data.

The following information illustrates the difference between values from your source data file and values that are added through hard-coded values:

- You have an Asset Family column in your source data file. The selection in the Source Field is %asset family%.
- You do not have an Asset Family column in your source data file. However, all of your assets are hardware assets. You specify a hard-coded value of Hardware in the Source Field.

  Note: You can also use the Main Destination Object to specify that all records in your source data file belong to a particular family or template. For example, the Asset (Hardware) selection for Main Destination Object specifies that all source records belong to the hardware asset family.

Multiple Values for a Single Field

You can add a mapping with multiple Source Field values that are mapped to a single Destination Field.

Example: Use multiple values for a single field

Your source data file has two columns with the names Manufacturer and Catalog Name. Combine these columns by selecting both in the Source Field. In this example, the Source Field selection is %Manufacturer% %Catalog Name%.

You can also enter multiple hard-coded values in the Source Field (for example, Document Management Company %model name% IT Department).

Filter Data in the Deletion Import

You can identify a subset of records in your source data file that you want to exclude from the deletion import. The Data Importer exclusion filter allows you to filter a part of your data source using exclusion filter rules.

Example: Define an exclusion filter to process returned assets

A CSV file that you receive from your hardware vendor includes assets that were ordered and returned to the vendor. You want to delete the assets that were returned to the vendor, so you want to process those records only. You define an exclusion filter to exclude records that do not have a status of Returned.

Follow these steps:

1. On the Administration tab, Data Importer page, Exclusion Filter area for a selected deletion import, select the Filter Type.

   And

   Excludes a record from the source data file only if all the rules that you specify are valid for the record.

   Or

   Excludes a record from the source data file if any of the rules that you specify is valid for the record.

2. Click New.
3. Click the Select icon next to Source Field, select a column from your source data file, and click OK.

   Note: The percent signs before and after the column name identify the name as a column from your source data file.

4. Select the Operator.

   Note: To specify "not equal to", select the "<>" operator.

5. Enter a Filter Value for the rule.

   Note: You can use special characters and wildcards in the filter value. The rules can process text, numeric, and date fields.

6. Click the Complete Record Edit icon.
7. (Optional) Click New and specify more exclusion filter rules.
8. Click Save.

   The exclusion filter rules are saved and are applied when the deletion import processes.

Submit the Deletion Import

To start a deletion import immediately, click Submit in the Schedule area of the page. The data source records from the data file for the selected deletion import are processed.

Note: You can specify a data file other than the default (from the Basic Information) if you want to use a different file.

You can also schedule the deletion import for a particular day and time. For more information, see schedule the deletion import (see page 203).

To view the import jobs for your current selected deletion import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

Schedule the Deletion Import

You can schedule a deletion import for a specific time and you can specify the interval for the deletion import (for example, daily or weekly). You can schedule multiple deletion imports to process simultaneously.

Follow these steps:

1. On the Administration tab, Data Importer page, in the Schedule area for a selected deletion import, select the Is Scheduled check box.
2. Provide the information for the schedule. The following fields require explanation:

   Run Time

   Specifies the time of the day, in 24-hour format, to process the deletion import. When you schedule imports, use the local time zone on the CA APM application server.

   Interval Day

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

   Data File

   Specifies a data file name other than the default (from the Basic Information) if you want to use a different file.

   If this file is available on the application server, you can search and select the file. If this file is not available on the application server, you can locate and upload the file.

   Upload Data File

   Browse for the source data file. This file is uploaded to the application server.

   First Run Date

   Specifies the date when the first deletion import starts to process.

   Interval Type

   Specifies the type of interval for the deletion import (for example, Day, Month, Quarter, Week, or Year).

Interval

Specifies how often the deletion import processes. This interval is based on the specified Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the import processes every two weeks.

Last Day of Interval

Specifies that the deletion import processes on the last day of the selected Interval Type. If you select this check box, any previous value that you added to the Interval Day field is removed, and the Interval Day field is disabled.

3. Click Submit.

   The deletion import is scheduled for the specified date and time.

Examples: Using the Schedule Settings

The following examples illustrate the use of the schedule settings.

- Select Day for Interval Type and 2 for Interval. The import processes every other day.
- Select Week for Interval Type, 1 for Interval Day, and 3 for Interval. The import processes every three weeks on the first day (Sunday) of the week.
- Select Month for Interval Type, 15 for Interval Day, and 2 for Interval. The import processes every two months on the 15th day of the month.
- Select Quarter for Interval Type and select Last Day of Interval. The import processes every quarter (every three months) on the last day of the last month in the quarter.
- Select Year for Interval Type, 1 for Interval Day, and 1 for Interval. The import processes on January 1 of every year.

To view the import jobs for your current selected deletion import, click Associated Jobs on the left side of the page. To view all import jobs for all imports, click Import Jobs. In the list of import jobs that appears, click Status Message to view the status of an import.

You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

View the Schedule Details

You can view the schedule details for a scheduled import job that you created.

First, open the list of import jobs.

- To view the scheduled import jobs for your currently selected import, click Associated Jobs on the left side of the page, select the Scheduled check box, and click Go.
- To view all import jobs for all imports, click Import Jobs on the left side of the page, select the Scheduled check box, and click Go.

In the list of import jobs that appears, click Schedule Details for a selected import.

View the Import Log Files

You can view the Data Importer log files to see the details of all CA-provided and user-defined imports that have completed. The Data Importer creates a log file for each import that you run, including imports that were submitted immediately or scheduled for a future time. All import activities are saved in the log files.

To view the log files, first open the list of import jobs.

- To view the import jobs for your current selected import, click Associated Jobs on the left side of the page.
- To view all import jobs for all imports, click Import Jobs.

In the list of import jobs, click View Logs for a selected import. If more than one log file is available (for example, for a scheduled import that has completed a few times already), all files are listed with their corresponding creation dates.

You can view any available LDAP Import Sync log file. If you click Start LDAP Data Import and Sync on the LDAP Data Import and Sync page (Administration, User/Role Management), an import job ID is displayed. Use this job ID to locate the job in the Data Importer list of import jobs. Then click View Logs for that job.

Note: You can also locate and view the import log files in the following location on the CA APM application server:

```
[ITAM Root Path]\Storage\Common Store\Import\Logs
```

Review the Import Log File - Best Practices

The Data Importer log file contains information and error messages regarding the processing of import jobs. To help you understand the results of your import and to troubleshoot any errors, use the information in this log file. This section contains some recommended best practices for working with the Data Importer log file.

Match the row number in the data file with the error message in the log file.

A log file error message identifies the corresponding row number from your data file. You can also find the data file row number in the row above or below the error message in the log file.

Sometimes the error message in the log file does not show the data file row number. In this situation, the actual data file values are shown immediately after the error message in the log file.

Count the number of error messages in your log file.

1. Search for the following phrases in your log file to find the error messages in the file. These phrases are included with the error messages.

   ```
   Web Service threw exception
   ```

   ```
   Error at record
   ```

2. After you find a type of error message, search for that error in the log file and count the number of occurrences.
3. Identify and search for more error types that appear in your log file and count the number of occurrences.
4. Compare the count of all errors in your log file with the statistics that the Data Importer generated for the associated import. To view these statistics, click Status Message on the Associated Jobs list or Import Jobs list. This comparison helps you account for all relevant errors and identify error messages that are not valid and can be ignored.

Verify that the Data was Deleted

You verify that your deletion import succeeded by viewing your data in CA APM and by reviewing the Data Importer statistics.

- **Review the Data Importer Statistics.** To review the statistics for your current selected deletion import, click Associated Jobs on the left side of the page. In the list of import jobs that appears, click Status Message for your import.

  You can also view the log file for more information about the import activity. In the list of import jobs, click View Logs for the selected import.

- **View the Data in CA APM.** To view the data in CA APM, navigate to the tab and subtab, if necessary, for the object that you deleted (for example, asset, company, or contact). Search for the objects that you deleted and verify that the objects are not available.

Example: Verify the Deletion of Laptops

After Miriam runs the deletion import, she performs the following steps to verify that the laptops were deleted:

1. Checks the import statistics.
   - Clicks Associated Jobs or Import Jobs on the left side of the Data Importer page.
   - Clicks Status Message for the deletion import and reviews the statistics.
2. Views the import log file and the user interface.
   - Clicks View Logs in the list of import jobs and reviews the contents of the log file.
   - Navigates to the Asset tab. Searches for the deleted laptops and verifies that the deleted laptops are not available.

Chapter 10: Managing Product-Provided Data Imports

This section contains the following topics:

Product-Provided Data Import Types

The product provides a set of predefined data imports that already contain all mappings and settings. These imports help you get started with data management. The two types of product-provided data imports allow you to perform the following functions:

- Read-only data imports–Allow you to monitor internal system functions, such as the LDAP Sync import of contacts.
- Object imports–Allow you to perform imports of common objects, such as locations, contacts, and assets.

You cannot modify the mappings and settings in the product-provided data imports. However, you can copy the imports and modify the copies.

Monitor the Status of Product-Provided Read-Only Data Imports

The read-only data imports perform internal system functions. You can monitor the status of the read-only imports, but you cannot submit these imports. You can copy the read-only imports and modify the copies to create your own imports.

Follow these steps:

1. Navigate to Administration, Data Importer.
2. Click one of the product-provided read-only data imports (not the object data imports). The following fields require explanation:

   CA APM - LDAP Sync Import

   Submits a data import with the data file that CA EEM generated. This data import creates contacts through the LDAP Sync component.

CA APM - Device Delete Import

Submits a data import with the data file that CA SAM generated. This data import deletes the information that is associated with deleted discovered assets.

CA APM - Device Insert or Update Import

Submits a data import with the data file that CA SAM generated. This data import adds or updates the information that is associated with discovered assets.

3. Click Associated Jobs on the left side of the page.
4. Click Status Message in the list of import jobs to view the status of an import.

Submit the Product-Provided Object Data Imports

The product-provided object data imports perform imports of common objects. You can submit these imports, and you can monitor the status of these imports. To submit a product-provided object data import, verify that data was added to the associated data files. You can also specify your own data file. However, the column headers in your data file must match the column headers in the product-provided data file.

You can also copy these imports and modify the copies to create your own imports.

Note: In a multi-tenanted environment, these imports add to or update the data in the Public Data tenant.

Follow these steps:

1. Navigate to Administration, Data Importer.
2. Click one of the product-provided object data imports (not the read-only imports). The following fields require explanation:

CA APM - Company Import

Creates and updates companies.

CA APM - Cost Center Import

Creates and updates cost centers.

CA APM - Location Import

Creates and updates locations.

CA APM - Contact Import

Creates and updates contacts.

Note: If you are using multi-tenancy, you cannot submit this import. Copy this import, add a mapping for the tenant, and submit your new contact import.

CA APM - HW Model Import

Creates and updates hardware models.

CA APM - HW Asset Import

Creates and updates hardware assets.

CA APM - Unreconciled Discovered Assets Import

Creates and updates discovered assets.

Note: A CA Business Intelligence report about unreconciled discovered assets provides input for this data import. This CA Business Intelligence report does not include the Class and Status fields. Add these fields to the data file that corresponds to this import.

3. Specify your own data file in the Schedule area or use the product-provided data file.

   Note: The product-provided data file does not contain data. Add the data that you want to import into the product-provided data file before you submit the import. You can find the product-provided data files at the following locations on the CA APM application server where the Storage Manager Service is installed.

   `[ITAM Root Path]\Storage\Common Store\Import`

4. Click Submit.

Chapter 11: How to Submit a Data Import Using the Command Line

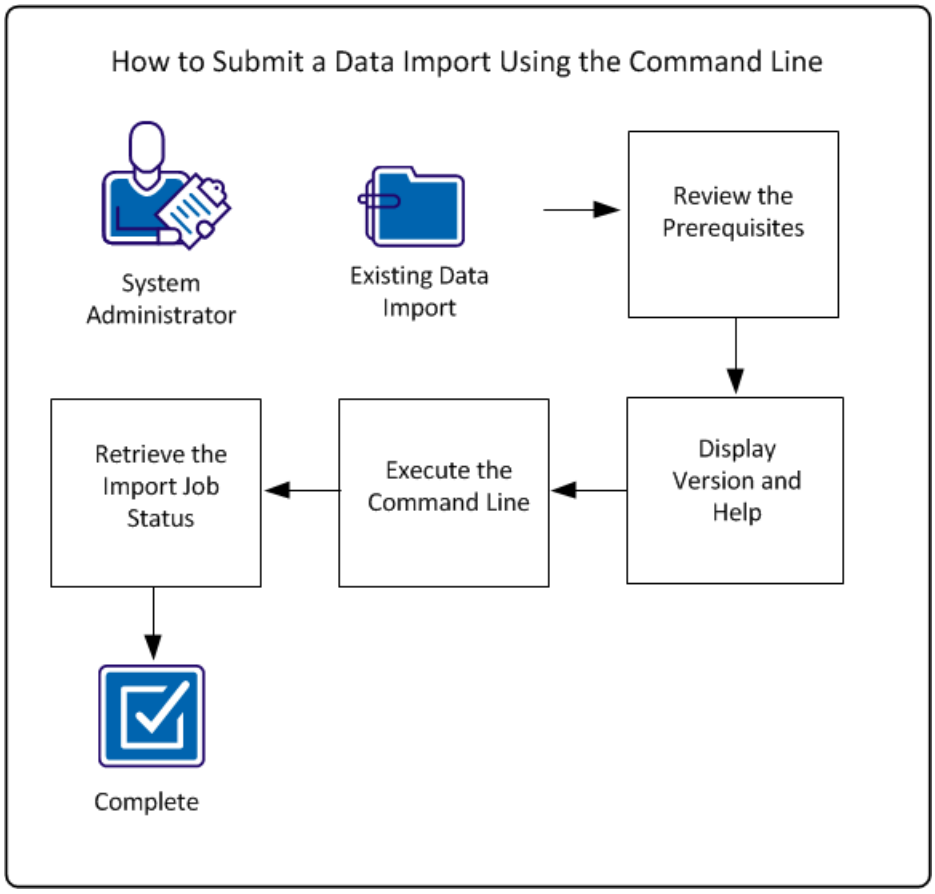
This section contains the following topics:

How to Submit a Data Import Using the Command Line

You can use a command line to submit a Data Importer data import for processing instead of using the CA APM user interface. You can execute the command line from the Import Processor folder on the application server where the product is installed. You can also copy the Import Processor folder to another computer. The users of that computer can then execute the command line, also.

The data import is submitted immediately and is executed by the Data Importer Engine with other import jobs from the CA APM user interface. You cannot schedule a data import to execute at a particular time using the command line. However, you can use a scheduler (such as the operating system scheduler) to specify dates and times to run the data import.

The following diagram illustrates how a system administrator submits a data import using the command line:



To submit a data import using the command line, perform these steps:

1. Review the Prerequisites (see page 215).
2. (Optional) Display Version and Help (see page 215).
3. Execute the Command Line (see page 216).
4. Retrieve the Import Job Status (see page 217).

Example: Import New Hardware Devices

Sam, the CA APM system administrator at Document Management Company, has an existing data import that adds new hardware devices to the data repository. Sam wants to execute that data import daily. Sam also wants to verify the status of the submitted import job. However, he does not want to log in to the product to perform the import because he does not always perform other product functions on a daily basis. Sam uses the command line to submit the data import and then verify the status.

Review the Prerequisites

To ensure that you can successfully submit a data import using the command line, verify that you have completed the following prerequisites:

1. Verify that Microsoft .NET Framework 4.0 is installed on the computer where you are executing the command line.
2. Define a data import with all mappings and settings through the CA APM user interface.
3. (Optional) If you change the Import Service URL, modify the ImportProcessor.exe.config file to reflect the new URL. You can locate the ImportProcessor.exe.config file in the Import Processor folder. Update the endpoint address value.

   Example: The following statements show an example of the endpoint address value that you modify to change the Import Service URL.

   ```
   <endpoint address="http://localhost/ImportService/ImportService.svc"
       binding="basicHttpBinding"
       bindingConfiguration="BasicHttpBinding_ImportService"
       contract="IImportService" name="BasicHttpBinding_ImportService" />
   ```

Display Version and Help

Specify the command line parameters to display the command line version and usage help.

Follow these steps:

1. Log in to the application server where you installed CA APM or to a computer that has the Import Processor folder.
2. Access the Import Processor folder.

   Note: On the application server, the Import Processor folder is located in the CA APM installation path.
3. Open a command prompt window and execute the following command:

   ```
   importerprocessor -H | -V
   ```

   -H

   Displays the command line version number and usage help for the command line parameters.

   -V

   Displays the command line version number.

Execute the Command Line

Specify the command line parameters to submit a data import.

Follow these steps:

1. Log in to the application server where you installed CA APM or to a computer that has the Import Processor folder.
2. Access the Import Processor folder.

   Note: On the application server, the Import Processor folder is located in the CA APM installation path.
3. Open a command prompt window and execute the following command:

   ```
   importerprocessor -usr "user_name" -pwd "password" -i "import_name"
   –df  "data_file_absolute_path" -t "tenant_name" –ts -c
   ```

   -usr

   Specifies the CA APM login user name.

   -pwd

   Specifies the CA APM login password.

   -i

   Specifies the name of the data import that was created previously through the CA APM user interface.

   -df

   Specifies the absolute path of the data file that is associated with the data import. The Data Importer Engine uses this file to process the import.

   -t

   (Required for multi-tenancy) Specifies the name of the tenant that is associated with the data import.

   -ts

   (Optional) Specifies that the command line parameters are recorded in the Import Processor log file.

   Note: The Import Processor log file is located in the Import Processor folder.

   -c

   (Optional) Identifies whether the data import was provided with the product or was created by a user.

   Valid values: 1 (product provided) or 0 (created by a user)

   Default: 0

Retrieve the Import Job Status

Specify the command line parameters to verify the status of an import job.

Follow these steps:

1. Log in to the application server where you installed CA APM or to a computer that has the Import Processor folder.
2. Access the Import Processor folder.

   Note: On the application server, the Import Processor folder is located in the CA APM installation path.
3. Open a command prompt window and execute the following command:

   `importerprocessor -usr "user_name" -pwd "password" -j "job_id" –ts`

   -usr

   Specifies the CA APM login user name.

   -pwd

   Specifies the CA APM login password.

   -j

   Specifies the import job ID.

   -ts

   (Optional) Specifies that the command line parameters are recorded in the Import Processor log file.

   Note: The Import Processor log file is located in the Import Processor folder.

Chapter 12: How to Submit a Data Import Using a Process Workflow

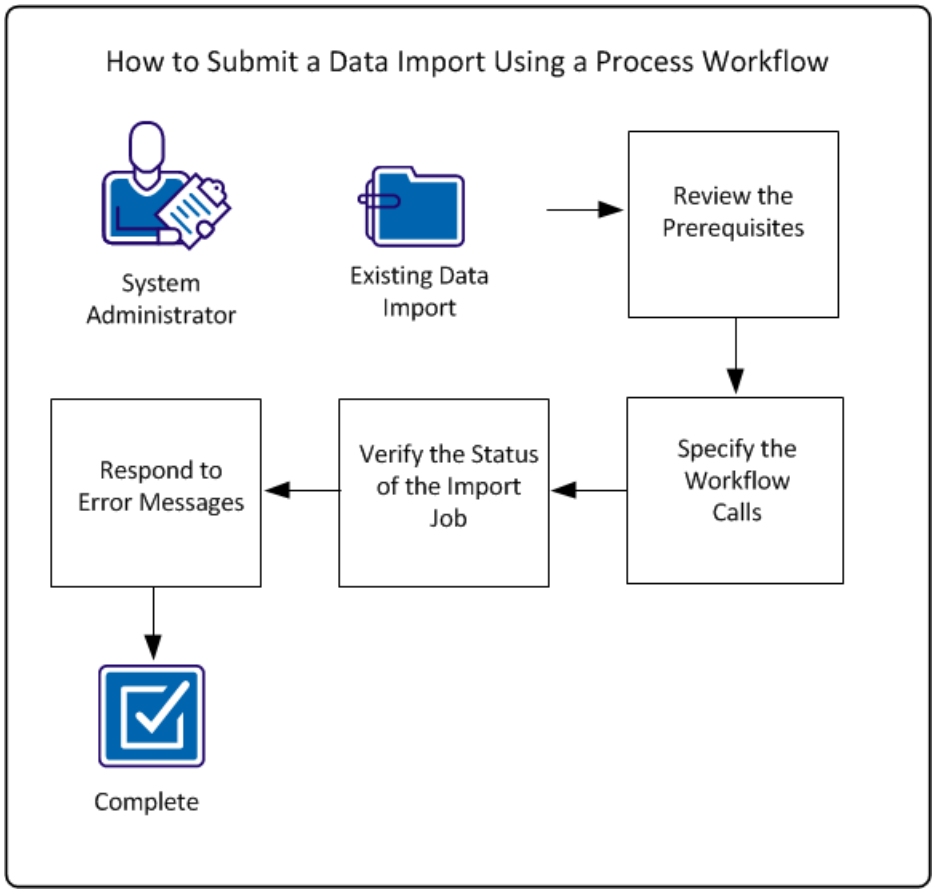
This section contains the following topics:

How to Submit a Data Import Using a Process Workflow

You can use a process workflow (for example, CA Process Automation) to submit a Data Importer data import for processing instead of using the CA APM user interface.

Note: You can create a data import process workflow using a company-provided sample XML file and integrating with CA Process Automation. For more information about this integration, see the *Implementation Guide*.

The following diagram illustrates how a system administrator submits a data import using a process workflow:



To submit a data import using a process workflow, perform these steps:

1. Review the Prerequisites (see page 221).
2. Specify the Workflow Calls (see page 221).
3. Verify the Status of the Import Job (see page 223).
4. (Optional) Respond to Error Messages (see page 224).

Example: Import New Hardware Devices through a Process Workflow

Sam, the CA APM system administrator at Document Management Company, has defined a business process workflow. The workflow discovers new hardware devices, adds the new devices to the company data repository, and runs reports about the new devices. Sam has already created a data import in CA APM that adds the new hardware devices to the data repository. Sam wants to execute that data import at a specific point in his overall workflow. He wants to integrate the data import with his overall business process workflow. Sam wants the data import to execute at the time that the workflow specifies without the user logging in to the product user interface. Sam updates his business process workflow to include calls to the CA APM web service operations for the Data Importer.

Review the Prerequisites

To ensure that you can successfully submit a data import using a process workflow, verify that you have completed the following prerequisites:

1. Define a data import with all mappings and settings through the CA APM user interface.
2. Verify that the data file path (if you are specifying a path) is accessible from the server where the Import Service is running. Also, the Network Service (application pool identity) user requires access to this path.
3. Define a process workflow using a workflow provider (such as CA Process Automation).

Specify the Workflow Calls

To launch the Data Importer and execute a data import from a process workflow, you provide specific workflow calls to CA APM web service operations. These operations perform the following functions:

- Login operation–Logging in to CA APM.
- Submitting a data import using one of the following ways of providing a data file:
  - SubmitImportwithfilepath Operation–The data file is available on a specified file path. This file path must be accessible from the server where the Import Service is running. The web service operation uploads the file.
  - SubmitImport Operation–The data file content has been converted to byte array binary format. The web service operation receives the byte array content from an application and submits the content to the Data Importer.

    Note: To use this way of providing a data file, create an application, if one is not already available, to convert the data file content to byte array format. The application then sends the content to the web service operation.

Incorporate the calls to these operations into your business process workflow.

Note: For information about creating a process workflow, see the product documentation for your workflow provider.

Login Operation

This operation logs in to CA APM using the specified CA APM user ID and password. The output of this operation is the login token. The login token is used as input to other data import workflow operations.

Input Parameters

ItamUserName–CA APM user ID

ItamUserPassword–CA APM user password

Output Parameters

loginToken–Token that is returned after the CA APM login.

SubmitImport Operation

This operation receives data file content that has been converted to byte array format and submits the content with the data import to the Data Importer. To use this operation, create an application, if one is not already available, to convert the data file content to byte array format. The application then sends the content to this web service operation.

This operation returns a data import job ID, which is used to verify the status of the import job.

Input Parameters

loginToken–Token that is returned after the CA APM login.

ImportName–Name of the data import.

Datafilename–Name of the data file that is associated with the data import.

Datafilestream–Data file content in byte array format.

Caprovided–(Optional) Indicator that specifies a product-provided data import. Set this parameter to one (1) to specify a product-provided import.

Tenant–(Multi-tenancy only) Name of the tenant to which the import applies.

Output Parameters

Job ID–ID that is returned after a data import is submitted successfully. The GetJobStatus operation uses this ID to verify the status of an import job.

SubmitImportwithfilepath Operation

This operation uploads a data file from a specified file path and submits the data file with the data import to the Data Importer. This file path must be accessible from the server where the Import Service is running.

The operation returns a data import job ID, which is used to verify the status of the import job.

Input Parameters

loginToken–Token that is returned after the CA APM login.

ImportName–Name of the data import.

Datafilepath–Complete path and name of the data file that is associated with the data import. This path must be accessible from the server where the Import Service is running. Also, the Network Service (application pool identity) user requires access to this path.

Note: If the data file location is a shared path, the CA APM server and the shared computer must be in the same domain.

Caprovided–(Optional) Indicator that specifies a product-provided data import. Set this parameter to one (1) to specify a product-provided import.

Tenant–(Multi-tenancy only) Name of the tenant to which the import applies.

Output Parameters

Job ID–ID that is returned after a data import is submitted successfully. The GetJobStatus operation uses this ID to verify the status of an import job.

Verify the Status of the Import Job

The Data Importer provides a status summary of each submitted data import job. Your process workflow can include a call to the CA APM web service operation that retrieves the status of a submitted data import job. Incorporate the call to this operation into your process workflow.

GetJobStatus Operation

This operation uses the data import job ID to verify the status of an import job.

Input Parameters

loginToken–Token that is returned after the CA APM login.

Job ID–ID that is returned after a data import is submitted successfully.

Output Parameters

Job Status–Status of the import job.

Respond to Error Messages

If errors occur during the data import workflow process, you can receive error messages. The following messages require explanation:

20002 – Cannot access the data import because of user permissions. Contact your administrator.

The user role requires Data Importer Admin access or Data Importer User access to submit a data import.

20005 – Cannot connect to the Import service. Contact your administrator.

Verify the Import Service URL in the ImportProcessor.config file, or contact your administrator.

21002 – The data import name is invalid.

The data import does not exist, or the user does not have access to the data import. If the data import is product-provided, specify a value of 1 for the Caprovided parameter.

21004 – The data file failed to upload.

This message can result from a configuration error. Review the Storage Manager Service log files.

21005 – No mappings are defined for the data import.

Define mappings and resubmit the data import.

22001 – The data import job ID is invalid. Verify the job ID and try to execute the import again.

Verify the job ID by logging in to CA APM and locating the data import job. Resubmit the data import with the valid job ID.

Glossary

allocation

An *allocation* is a description of how your organization is internally approved to use a particular software product, as specified in your software license. Some examples of an allocation are enterprise, single-user, and single-server.

allocation relationship

An *allocation relationship* is a record that provides the attributes of a software internal allocation. Each allocation relationship provides attributes and relationships that apply to a particular type of allocation.

asset

An *asset* is an IT product that you own or are about to acquire. Assets represent physical products with unique identifiers such as a serial number, a configuration, or a contact. You define an asset record for each asset that you want to track individually.

asset configuration

An *asset configuration* is a record that describes the configuration of a hardware asset as it currently exists in your environment. Asset configurations are different from model configurations due to changes made over time.

asset family

An *asset family* is a way to organize and classify assets to track specialized information about products, services, or equipment used in your organization. The asset family determines the information that you see on the page when you define an asset. Asset family was previously named asset type.

asset group

An *asset group* is a related set of assets that share information. Information is tracked only for the group and not for individual members of the group.

attachment

An *attachment* is an electronic file or URL page that contains supporting documentation for an object. For example, you can attach a scanned contract with a legal document to represent the contract.

audit history

An *audit history* is a chronological list of changes made to an object record over time.

change event

A *change event* monitors field changes for an object and works with notifications that are created by a workflow provider (for example, CA Process Automation) to notify you that the field value has changed.

class

A *class* is a broad descriptive category of an asset family that is assigned to a model or asset and facilitates information retrieval.

company

A *company* is an organization that manufactures, sells, or purchases products tracked in your repository or is a party to legal documents tracked in your repository.

configuration

A *configuration* has two specific definitions within CA APM. A configuration can be a description of a computer (such as a PC, laptop, server, and so forth) and its individual components (monitor, modem, and so forth). You use configuration records to identify models and assets that represent a computer's components. A configuration is also a method to change the user interface and default behavior of the product so users can more easily enter, manage, and search for information.

configuration relationship

A *configuration relationship* is the set of attributes that belong to a particular category of hardware configurations. Configuration relationships are provided for assets and models.

contact

A *contact* is a person or department that is involved with the acquisition, use, or management of an object in your repository.

date event

A *date event* monitors date field changes for an object and works with notifications that are created by a workflow provider (for example, CA Process Automation) to notify you that an important date is approaching or has passed.

escalation

An *escalation* is the process of automatically forwarding a notification to another person after the original recipient does not respond within a given time period.

escalation cap

An *escalation cap* is an upper limit on the amount a recurring cost can increase. Typically, contracts specify the limit.

escalation percentage

An *escalation percentage* is an amount by which you expect a recurring cost that is associated with an asset or legal document to increase each recurring period. For example, you have a $100 charge that recurs once a year for three years. To account for inflation, you expect a vendor to increase product costs by 5 percent each year. The cost of the product would be $100 for the first year, $105 for the second year ($100 + (.05 x $100) = $105), and $110.25 for the third year ($105 + (.05 x $105) = $110.25).
The escalation percentage is based on the recurring period. If you make monthly payments, but the amount due is likely to increase on a yearly basis, you can enter the cost as a yearly cost with an escalation percentage. A yearly payment is calculated, increased by the escalation percentage every year until the termination date.

Event Server

The *Event Server* is a product component that processes events. The server periodically scans event tables in the repository and fires the event when the event occurs. After firing the event, the workflow provider sends notifications to users and manages acknowledgements. The server updates the repository with the information so you can determine whether the workflow process is completed, in progress, failed, or aborted.

extended field

An *extended field* is a field that can be added to any object record. Extended fields can be used to store information that you need to track about an object not provided by a default field.

governing legal document

A *governing legal document* is the document on which a legal document is based. The governing legal document has the main set of terms and conditions from which the legal document is derived.

item

See *model*.

legal document

A *legal document* is a document that describes a legal relationship or agreement between two or more parties. For example, contracts, notification letters, master agreements, leases, volume purchase agreements, letters of intent, and so on are all considered legal documents. Although software licenses are legal documents, they are tracked differently.

legal template

A *legal template* is the set of attributes that belong to a particular category of legal documents (for example, all leases have start dates, end dates, lessors, and lessees). These attributes include terms and conditions that typically apply to that category and user fields.

location

A *location* is the physical place where an asset, a company, or a contact is found.

masking

Masking is a way to specify search criteria in which you substitute one character for part of a character string. Masking characters are also known as *wildcard characters*. Use masking to limit the number of records returned by a search or to substitute for search characters when you do not know the exact spelling.

match values

Match values are key fields that uniquely identify entities within a database. For a hardware asset, the match values would be the combination of Domain ID, Unit ID and Type, which uniquely identify a row in the UNIT table.

model

A *model* is a record that describes a product that you may have purchased in the past or may possibly purchase in the future. Model was previously named item.

model configuration

A *model configuration* is a record that describes the standard configuration that you purchase for a particular hardware model.

multi-tenancy

Multi-tenancy is the ability for multiple independent tenants (and their users) to share a single product instance (for example, CA APM). Multi-tenancy lets tenants share hardware and application support resources, reducing costs while gaining most of the benefits of an independent implementation. Tenants can only interact with each other in defined ways; otherwise, each tenant views the application instance as solely for its own use.

normalization

Normalization is part of the reconciliation process where you establish a list of rules to standardize, organize, and consolidate data between CA APM and discovered repositories.

note

A *note* is text that is added to an object record to add more detailed information.

notification

A *notification* is created by a workflow provider (for example, CA Process Automation) to communicate information to your team members about important events and activity.

object

An *object* represents something that you record and track in your repository. The primary objects in CA APM are models, assets, legal documents, contacts, companies, organizations, locations, and sites.

parent company

A *parent company* is a company that owns or controls another company (its subsidiary company).

parent tenant

To place a tenant into a hierarchy, you assign it a *parent tenant*. The parent tenant becomes the tenant immediately above that tenant in a hierarchy. To remove a tenant from a hierarchy, you can remove its parent tenant assignment.

payment schedule

A *payment schedule* is a list of payments to be made for a particular cost record. Information in the payment schedule includes when a payment is due, the amount due, whether a payment was made or approved, and in what amount. The information you provide on the Cost page is used to calculate the payment schedules. If you define the recurring period details, the system auto-creates payment records in the database based on the recurring period details you define.

preferred vendor/preferred seller

A *preferred vendor/preferred seller* is the seller company that you prefer to use for future acquisitions of a product.

recurring cost

A *recurring cost* is a cost that repeats for a certain time period. Recurring time periods are based on the terms of your agreement. Do not confuse the length of the recurring period with the frequency of payments. For example, if a cost recurs yearly for three years, specify three years as the recurring cost even if you make payments on a monthly basis. You can change the payment frequency at a later time.

related tenants group

A *related tenants group* is a tenant group that includes a tenant and all tenants belonging to its *subtenant group* or its *supertenant group*.

relationship

A *relationship* is an association between a managed object and another object. Relationship records provide detailed information about the association.

relationship record

A *relationship record* is created when a primary object is linked with one or more secondary objects.

relationship template

A *relationship template* is the set of attributes that belong to a particular category of relationship. These attributes determine what types of objects can be linked to each other and the nature of those links.

reminder

A *reminder* is a notification triggered by an event that alerts a user about an important event or activity.

role

A *role*, used in security, is a group of users who perform the same tasks and who require the same levels of access to data or functionality.

service provider

The *service provider* is the master tenant (owner) of a product instance. A product instance can have only one service provider, which can also participate as a parent in one or more tenant hierarchies.

start request form

A *start request form* is a CA Process Automation automation object that allows users to request the initiation of a new workflow process. A start request form creates an interface that lets users provide structured input and launch a process.

subclass

A *subclass* is a descriptive category of a class that is assigned to a model or asset to further refine the description provided by the class.

subsidiary company

A *subsidiary company* is a company that is owned or controlled by another company (its parent company).

subtenant

A *subtenant* is a tenant that is lower than another tenant (its relative *supertenant*) in the same tenant hierarchy. Subtenants can be departments or sites within their supertenants. Subtenants can have their own business rules and data, and they also share some business data with their parent tenant and higher supertenants.

subtenant group

A *subtenant group* is a tenant group that includes a tenant, its subtenants, their subtenants, and so on, to the bottom of that hierarchy. As long as a tenant resides in a hierarchy, its subtenant group is product-maintained; only its name and description can be modified.

supertenant

A *supertenant* is a tenant that is higher than another tenant (its relative *subtenant*) in the same tenant hierarchy.

supertenant group

A *supertenant group* is a tenant group that includes a tenant, its parent tenant, and so on, to the top of that hierarchy. As long as a tenant resides in a hierarchy, its supertenant group is product-maintained; only its name and description can be modified.

template

A *template* provides pre-defined groups of fields that are associated with a specific object type. For example, a legal template provides fields that belong to a particular type of legal document.

tenant

A *tenant* is one instance among multiple instances of a single product installation. Using tenants, CA APM can manage multiple separate enterprises that provide support to customers. Each tenant has unique settings and properties and sees the product as its own application, except when the tenant shares data through *service provider* authorization or a *tenant hierarchy*.

tenant hierarchy

A *tenant hierarchy* is a tenant group that you define and manage when you define subtenants (that is, you assign them parent tenants for organizational or data sharing purposes). CA APM supports tenant hierarchies of unlimited depth. However, the service provider can limit the total number and depth of tenants in a hierarchy. The service provider also can prevent individual tenants from having subtenants.

terms and conditions

Terms and conditions specify the areas of agreement for legal documents. Before you define a legal template, create a single master list of all terms and conditions that can be assigned to a legal template. A term and condition can be assigned to multiple legal templates and legal documents.

trimming

Trimming is a way to specify a fixed number of leading or trailing characters to ignore on an asset when performing hardware reconciliation. For example, discovered computer names at one site have a three-character location code as a prefix. You create a trimming record for the asset matching criterion that trims three characters from the left side of the discovered computer names.

watch event

A *watch event* monitors field changes for an object and works with notifications that are created by a workflow provider (for example, CA Process Automation) to notify you about a potential obstruction to completing a task.

workflow provider

A *workflow provider* manages notifications and acknowledgements for events.