CA Asset Portfolio Management

User Guide

Release 12.9.00

CA Technologies Product References

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

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

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

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

- Common Asset Viewer

  (formerly Asset Management System or AMS)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Introduction

This section contains the following topics:

Overview

CA APM provides asset portfolio management capabilities to help you manage technology assets that you own, lease, or license. The product helps you optimize your IT asset investments and avoid overspending by enabling a portfolio view of your IT asset costs, contracts, and licenses. This view allows you to manage and control costs to make more informed business decisions. The product helps you identify unused and under-utilized assets to help you increase and optimize asset use and reduce overpayment on invoices. CA APM helps you manage your IT assets throughout their lifecycle, from initial planning and purchase to retirement and disposal.

CA APM unifies and simplifies the management of assets and helps you in the following ways:

- Understand the assets that you own and lease, and the cost of owning the assets so that you do not purchase assets that you do not need. You can optimize your assets, fully leverage existing usage rights, and redeploy unused licenses.
- Understand who uses the assets, and the total number of available assets.
- Understand your maintenance contracts for hardware and software assets. You can review and cancel unnecessary contracts, and revise existing contracts to control costs.
- Understand when an asset reaches the end of a lease to help control costs and negotiate better contracts.
- Monitor your vendors and contracts to improve vendor negotiations.
- Improve asset approvals and fulfillment, and increase efficiency by automated processes.

Audience

This guide is intended for anyone who uses the product on a daily basis to manage the financial and ownership information of IT assets, including the following users:

- *IT Asset Managers* implement and manage the overall asset management system and work directly with various departments such as finance and procurement.
- *Finance and Procurement Managers* develop and implement procurement systems, including order processing and the deployment of IT hardware and software assets.
- *Contract, Leasing, and Vendor Managers* negotiate, review, and maintain contracts, agreements, and services under contract. Common tasks include requesting quotes from vendors and negotiating product prices, delivery dates, and purchases.
- *Operations Managers and Discovery Specialists* manage the IT infrastructure and the deployment and implementation of IT asset discovery tools and techniques.
- *Help Desk Manager/Analyst* plan, direct, and administer the help desk to ensure that assets are properly deployed and maintained. Any asset requests reported to the help desk are recorded, processed, and resolved based on departmental policies and procedures.

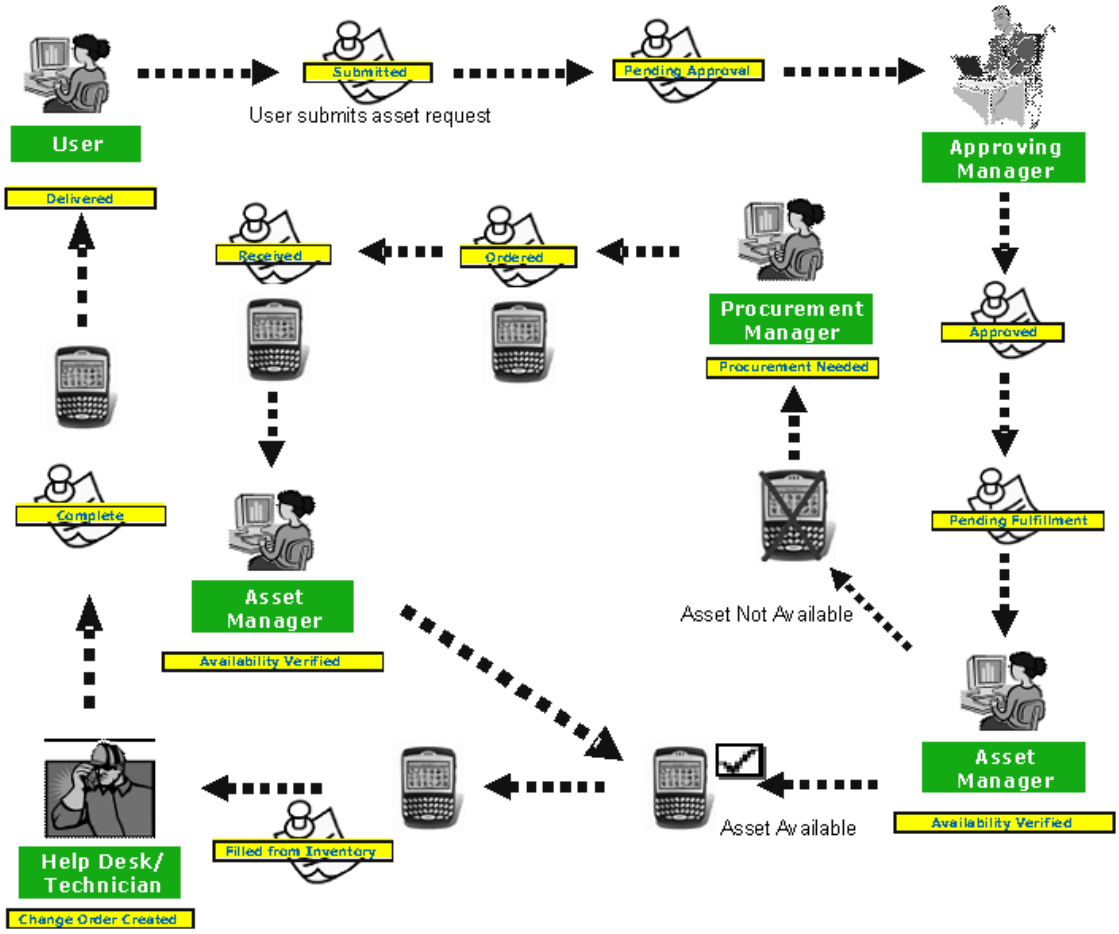
Log In to CA APM

After the product is installed, your CA APM administrator prepares the product so that you can use it on a daily basis to manage assets. After your administrator prepares the product, they will provide you with the URL and login credentials for you to log in.

The Asset Request Lifecycle

When you integrate CA APM and CA Service Catalog, you help improve the quality of service, increase efficiency, and streamline and automate asset approvals and fulfillment.

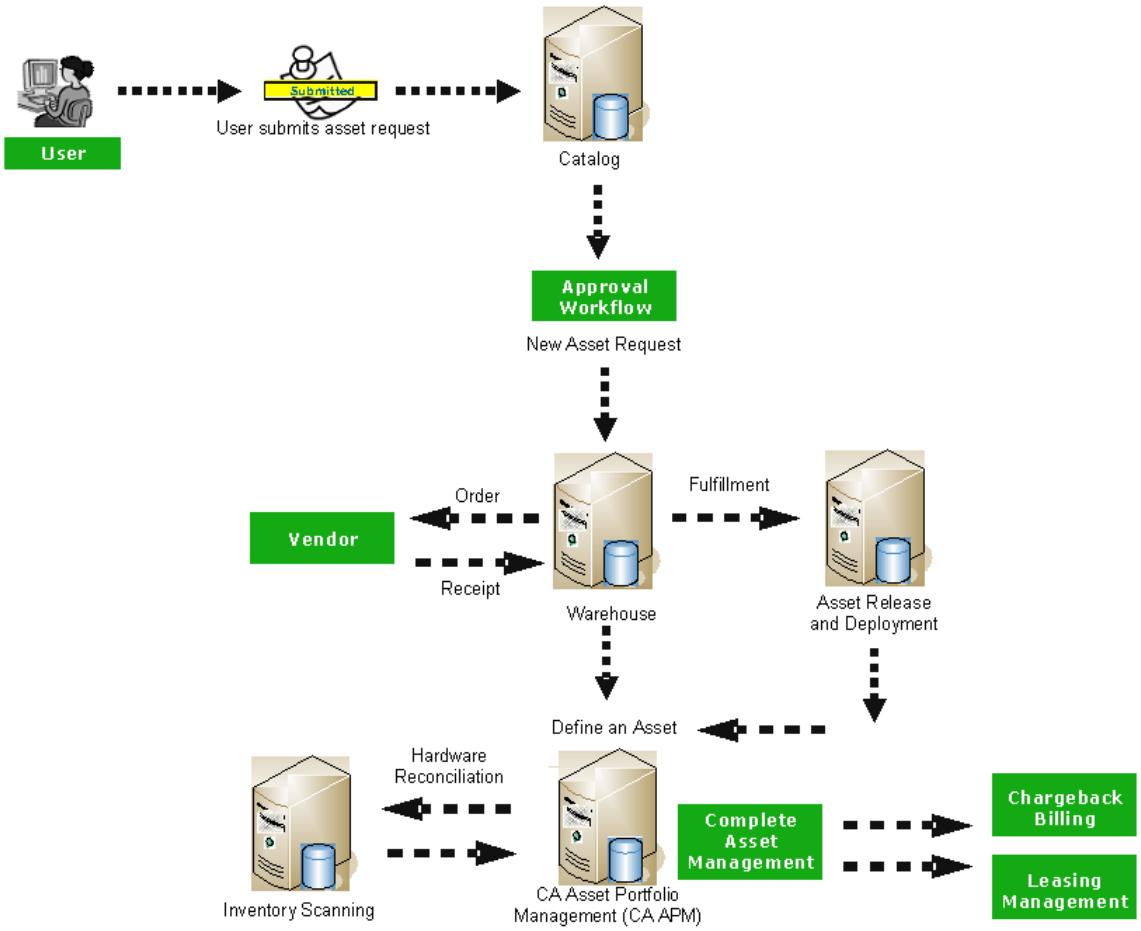
As shown in the following illustration, the CA APM integration with CA Service Catalog helps to automate all aspects of the asset request lifecycle.



The Asset Lifecycle

CA APM provides complete asset portfolio management capabilities to help you manage technology assets that you own, lease, or license. CA APM provides you with features to help you manage your IT assets throughout their lifecycle, from initial planning and purchase to retirement and disposal.

As shown in the following illustration, CA APM provides complete management capabilities for all aspects of the asset lifecycle.



Example: Asset Management

To help you understand how CA APM can help you manage your assets, the following examples are provided. These examples use a fictional sample corporation (Document Management Company) to help you understand how CA APM and the following products integrated with CA APM simplify asset management:

- CA Service Catalog
- CA Service Desk Manager
- CA Asset Inventory Manager

Important! Document Management Company is a fictitious company name which use is strictly for instructional purposes only and is not meant to reference an existing company.

To understand the benefits of using CA APM, read the examples in the order provided.

Note: In the examples, specific tasks are presented in which you must use a particular CA Technologies product to perform the task. For example, you use CA Service Catalog to fulfill a request from inventory. These examples do not include the step-by-step instructions to complete the task. Read your product-specific documentation for that information.

Example: How to Request a Laptop

The following example illustrates how Document Management Company uses the integration between CA APM and CA Service Catalog to review existing inventory and determine whether to purchase a new laptop, or reallocate an existing laptop. When Document Management Company knows how many laptops that they own or lease, they can reduce their risk of purchasing or leasing a laptop that they do not need. Instead of purchasing a new laptop, they reallocate an existing laptop. As a result, their cost of ownership decreases.

This integration provides Document Management Company with the following benefits:

- They do not purchase a laptop that they do not need.
- The process that is used to request a laptop is automated and is available to all users, reducing the purchasing cost.
- Inventory within Document Management Company is tracked so that they can allocate and redeploy an existing laptop, rather than purchase a new laptop.

To request a laptop, complete the following steps:

1. Create a request for the laptop in CA Service Catalog and submit the request for approval.

   The sales manager hires a new sales administrator, and the manager must provide the sales administrator with a laptop. The sales manager uses CA Service Catalog to review the catalog for the available laptop inventory and configurations, select an existing laptop, review the request to see associated costs, and submit the request for approval. The sales manager specifies that the laptop must be available by June 1.

2. Review the request status in CA Service Catalog.

   The sales manager periodically reviews the request to see the status, any changes, and to determine how far along the request has progressed in the process. The request is automatically sent to the vice president of sales for approval.

3. Approve the request in CA Service Catalog.

   The vice president of sales receives an email indicating that the laptop request must be approved. The vice president of sales reviews the request to verify that the costs associated with the laptop are within the guidelines for the management team. The request is within the guidelines, and the vice president of sales approves the request. The request is automatically sent to the asset manager for approval.

4. Approve the request in CA Service Catalog, review available inventory in CA APM, and fulfill the request.

   The asset manager receives an email indicating that the laptop request must be approved. The asset manager reviews the request and reviews the available inventory in CA APM to see if there is an available laptop. A laptop matching the requested configuration is available from inventory, and the asset manager fulfills the request for the laptop.

5. Assign the laptop ownership in CA APM.

   The asset manager finds a laptop in CA APM matching the configuration in the request. The sales administrator is not yet an employee, so the asset manager assigns the ownership of the laptop to the sales manager.

6. Review the request status in CA Service Catalog and verify that a change order exists.

   The asset manager reviews the original request in CA Service Catalog to verify that the request is fulfilled from existing inventory. The asset manager also verifies that a CA Service Desk Manager change order is created and is sent to the help desk analyst to prepare the laptop for the sales administrator.

7. Review and complete the change order in CA Service Desk Manager.

   The help desk analyst receives an email indicating that a change order for the laptop must be completed. The help desk analyst reviews the change order details, including allowing the analyst to see the original request in CA Service Catalog. The help desk analyst uses the information in the change order to configure the laptop for the sales administrator. The help desk analyst adds comments to the change order to indicate the work performed, and approves the change order so that the change order status is closed.

8. Deliver the laptop.

   The help desk analyst configures and prepares the laptop, and delivers the laptop to the sales administrator.

Example: How to Redeploy a Laptop

The following example illustrates how Document Management Company uses the integration between CA APM and CA Asset Inventory Manager to collect and redeploy a laptop after an employee leaves the company. When Document Management Company knows how many laptops that they own and lease and properly manage their assets, they can verify that all assets are collected and reallocated properly.

This integration provides Document Management Company with the following benefits:

- They do not purchase a laptop that they do not need.
- The process that is used to reallocate a laptop is automated and is available to all users.
- They can make better purchasing decisions and reduce the risk involved when purchasing assets.

To redeploy a laptop, complete the following steps:

1. Review all assets in CA APM that are assigned to the employee.

   The asset manager logs in to CA APM and reviews all assets that are assigned to the employee. The employee has three assigned assets: a Blackberry, a security card, and a laptop.

   By reviewing all of the information about the laptop, the asset manager can decide how to redeploy the laptop. For example, the asset manager can see that the laptop was purchased for a particular cost center. Based on this information, the asset manager knows that the laptop cannot be deployed to an employee in a different cost center.

2. Review the discovered information about the laptop in CA Asset Inventory Manager.

   CA APM and CA Asset Inventory Manager are integrated, and the asset manager uses CA Asset Inventory Manager to review the discovered information about the laptop. By reviewing the discovered information, the asset manager can see that the laptop was purchased with 2 GB of memory and was upgraded to 4 GB of memory. The asset manager also reviews the storage capacity and software installed on the laptop to determine if an upgrade is necessary.

3. Review the laptop details in CA APM.

   The asset manager uses CA APM to review the following information about the laptop:

   - Support contact information when there are issues with the laptop. The laptop also has 48 hour support resolution in CA Service Desk Manager.
   - Costs associated with maintaining the laptop. Document Management Company has a lease on the laptop and is paying $34 a month until 12/31/2011. This information is useful to validate any vendor invoices for the laptop and to verify that the vendor is charging the correct amount. This information also allows the asset manager to understand future spending for the laptop.
   - Configuration components added to the laptop. The laptop is leased, and the asset manager must understand what components have been added. This information helps prevent the laptop from being returned to the vendor with components that have been paid for.
   - Lifecycle of the laptop. The asset manager can see that the laptop was ordered and received in November of 2008, and deployed in December 2009.
   - Audit history to review changes made to the laptop. By reviewing the audit history, the asset manager can see all changes, when the changes were made, and who made the changes.
   - Software internal allocations. The asset manager reviews the contact allocation for the laptop to determine if the software licenses can be made available for another user.

4. Redeploy the laptop.

   The asset manager reviews the information about the laptop and the associated contractual obligations. The lease for the laptop has not ended, and ending the lease is not an option because of the penalties involved. Therefore, the asset manager redeploys the laptop to another employee.

Example: How to Manage a Contract

The following example illustrates how Document Management Company uses CA APM to meet their contractual obligations to their vendors. When Document Management Company has all of the information about their contracts, they can determine what company is associated with the contract, who negotiated the contract, the costs associated with the contract, the length of the contract, and the assets associated with the contract.

This information provides Document Management Company with the following benefits:

- Helps to reduce the cost of owning an asset.
- Helps to make better purchasing decisions.
- Helps to reduce the risk involved in purchasing assets.

To manage a contract, complete the following steps:

1. Review the legal documents in CA APM to investigate potential consolidation and savings for hardware contracts.

   The contract manager logs in to CA APM and reviews the termination fees associated with all contracts. Termination fees are one time costs that Document Management Company must pay to discontinue any hardware contract.

2. Review the contract details for the legal documents to determine which agreements offer a lower penalty.

   The contract manager reviews the contract start date, end date, cost center, location, negotiator, and original requester. This information is important to verify because contracts may have been signed many years before the current date.

3. Review the costs associated with the contract.

   The contract manager reviews the costs to verify whether the vendor is billing correctly, and to determine the total amount paid for the contract and future payments. The information can be used for budgeting and forecasting.

4. Review the status history for the contract.

   The contract manager reviews the various stages of contract review (internal and external) to determine whether important changes occurred from the time the contract was signed and executed.

5. Review the audit history of the contract.

   The contract manager reviews the audit history of the contract to see all changes, when the changes were made, and who made the changes.

6. Review the terms and conditions for the contract.

   Canceling a contract, especially a lease, can have a large financial impact on Document Management Company. All assets must be returned to the vendor and new assets must be provided to employees. The contract manager reviews the terms and conditions, and determines that it is cost prohibitive for Document Management Company to cancel the lease.

7. Review a scanned document of the original contract.

   The contract manager reviews a scanned document of the original contract to perform a thorough review of the contract.

8. Review any additions, amendments, and governing legal documents that are associated with the contract.

   The contract manager reviews any additions, amendments, governing legal documents, and other associated attachments to the contract to improve purchasing decisions.

Example: How to Manage a Lease

The following example illustrates how Document Management Company uses CA APM to track and manage laptops assigned to a specific lease contract. When Document Management Company has all of the information about their leased assets, they can understand when a lease expires, understand the original lease configuration, understand where the leased assets are located, and understand the payments associated with the lease.

This information provides Document Management Company with the following benefits:

- Helps to reduce the cost of continuing a lease (possibly at a higher rate).
- Help to reduce the risk of buying out a lease (paying the full amount of the asset) if the asset cannot be found.

To manage a lease, complete the following steps:

1. Review the legal documents in CA APM.

   The asset manager has asked the asset administrator to provide an overview of the laptops in which the lease is expiring over the next three months. The information helps plan for the arrival and deployment of new laptops and servers.

2. Review the lease contract.

   Document Management Company leases laptops from Dell, and the asset administrator searches for all contracts from Dell. Two active contracts exist, and the asset administrator reviews the following information about the leasing contract:

   - Terms and conditions. As a best practice, match the terms and conditions with the words used in the contract. When terms and conditions are used in this way, Document Management Company can review and search legal documents for specific items.
   - Start and end date
   - Internal contact

3. Review the asset information for the laptops that are associated with the lease contract.

   The asset administrator reviews the asset information and can see that the laptops were purchased with 2 GB of memory, the employee to which each laptop is assigned, and where each laptop is located.

4. Review the discovered information about the laptops in CA Asset Inventory Manager.

   CA APM and CA Asset Inventory Manager are integrated, and the asset administrator uses CA Asset Inventory Manager to review the discovered information about the laptops. The asset administrator can see that a specific laptop in the lease was purchased with 2 GB of memory and has been upgraded to 4 GB of memory. The asset administrator also reviews the storage capacity and software that is installed on the laptops to determine if an upgrade is necessary. The asset administrator also reviews the added components to help prevent the return of a laptop to the vendor for components that have been paid for.

5. Search for all laptops related to the Dell lease in CA APM.

   The asset administrator searches for all laptops related to the Dell lease, and can see all of the leases that are scheduled to end, where the assets are located, the contact, and the specific end date.

6. Export the search results to a CSV file in CA APM.

   The asset administrator exports the lease information to a CSV file and send the information to the asset manager.

Chapter 2: Financial Management

This section contains the following topics:

Financial Management

Understanding the financial impact of your asset base lets you decide what costs are relevant to your business. CA APM helps you track, manage, and categorize all asset-related expenditures, including historical, current, and projected costs, so that you can analyze their financial impact.

Financial management in CA APM involves working with the following objects:

- Models (see page 23)
- Assets (see page 27)
- Asset Configurations (see page 40)
- Costs and Payments (see page 43)
- Events and Notifications (see page 46)
- Notes (see page 75)

Models

The repository contains two types of records that describe the basic characteristics of IT products:

- A *model* describes a product type that you have purchased or might purchase.
- An *asset*, which is based on a model, describes a product that you own or plan to acquire. You can create many assets that are based on a single model, and the new asset inherits the model attributes. For example, if you own 100 laptops of a particular model, you would have one model record describing the laptop and 100 asset records describing the individual laptops.

A model can be any of the following examples:

- A *computer model* such as Dell Optiplex GX270 and Dell Precision 410.
- A *hardware component* such as 104+ keyboard, 256 MB-RAM, Monitors, and Intel Pentium processor.

You manage *hardware models* to describe the following models:

- Configurations that the manufacturer offers.
- Substitutions or additions that you typically make to the configurations when you purchase them.

Each model configuration is composed of links between the models and their component model records (such as a monitor and a keyboard).

You can have some products that you want to group together to manage as models, such as the following examples:

- Standard, relatively inexpensive computer components in a configuration. For example, you can record a particular type of network card as a model. This model lets you determine which systems are using that type of network card without tracking details about individual network cards of that type. Other similar components include SCSI hard drives, memory, graphics cards, and CD or DVD devices.
- Products that your company purchases from different vendors at different times. This additional information lets you track pricing information for those products and select the best price.

Define models first in the repository for each asset that you want to manage. After you define a model, the model acts like a template for the physical assets that are created. The assets inherit the properties or attributes from the model, such as the name, asset family, and manufacturer. By using this template, a single model can represent many assets and the model information is common to many assets. However, each asset record contains information specific to that asset.

Manage Models

Managing models includes defining, updating, and deleting models for an asset. For example, you define Dell Precision Workstation 410 as a model to describe the workstation.

Follow these steps:

1. Click Model.
2. Perform one of the following actions.

3. **Define a model.**
   a. Click New Model.
   b. Enter the model information.

   Note: You can also define a model by copying an existing model, supplying a new name, changing the model information, and saving the new model.

4. **Update a model.**
   a. Search for the list of available models.
   b. Click the model that you want to update.
   c. Enter the new information for the model.

   Note: You can also view the details for an object that is related to your model, if the related object has a Browse icon. When you click the Browse icon, you leave the model page and you navigate to the related object page. To keep the model page in view and preserve the model information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.

5. **Delete a model.**
   a. Search for the list of available models.
   b. Click the model that you want to delete.
   c. Click Delete and confirm that you want to delete the model.

6. Click Save.

Define an Asset from a Model

You define an asset, which is based on a model, to describe a product that you own or plan to acquire. For example, you have defined Dell Precision Workstation 410 as a model. Your enterprise has purchased 100 individual computers, and you define 100 asset records that are based on the model to describe the individual computers.

Note: You cannot define an asset from a model that does not have an asset family.

Follow these steps:

1. Click Model, New Model.
2. Enter the model information with a valid asset family.
3. Click Save.

   The model is defined.

4. Click the Create Asset hyperlink.

5. Enter the asset-specific information.
6. Click Save.

Make an Obsolete Model Inactive

As a best practice, change the status of an obsolete model to inactive rather than deleting the model. For example, after replacing all Dell Precision Workstation 410 computers with laptops, you can change the status of the associated model to inactive.

We recommend this approach because deleting a model record permanently removes the historical information from the repository. Changing the status to inactive lets you retain the model information for future reporting and reference.

Note: Changing the status to inactive has no impact on the assets that are based on the model. If you want the assets to be inactive, search for the assets that are based on the model and manually indicate that they are inactive.

Follow these steps:

1. Click Model and search for the list of available models.
2. Click the model that you want to make inactive and select the Inactive check box.
3. Click Save.

Change a Model Asset Family

You can change the asset family of selected models. For example, you realize that a set of related computer models were imported into the product using the hardware asset family. You search for these models and select them. Then you can change the asset family for all selected models simultaneously.

Note: When you change the asset family for a model, the asset family is also changed for the associated assets.

Follow these steps:

1. Click Model.
2. Click Change Model Asset Family under Mass Change Utilities on the left.
3. Select the original asset family and the new asset family.

   Note: If the original asset family has extended fields that the new asset family does not have, a warning message and a check box appear. To proceed with changing the model asset family, select the check box Check to change model to new asset family. The extended fields are lost. To avoid the data loss, define the extended fields for the new asset family before you change the model asset family.

4. Click Go.

   All models that have the original asset family are listed in the Search results.

5. Select either the individual models that you want to change or all models.
6. Select a class for the models using one of the following actions:
   - Select the Assign a Single Class to All Models check box and select a class if you want to apply the same class to all selected models.
   - Select the class for each individual selected model.
7. Click Change Model Asset Family.

   Your request is submitted.

8. Click View Mass Change Utilities Progress to see the status of your job and verify completion.

Add Components in a Model Configuration

You associate a hardware model to its component models to define a model configuration. A generic model is a model that is not acquired as an asset, for example, keyboards and network cards. Generic models comprise a model configuration. This configuration is available to the inherited assets from the model.

Follow these steps:

1. Click Model and search for the list of available models.
2. Click the model for which you want to add components.
3. Expand Configurations on the left and click Model Configuration.
4. Click Select New, search for and select a model.
5. Click the Edit Record icon next to the model name to define the association between the hardware model and model components.
6. Click Save.

Assets

An *asset* is an IT product that you own or plan to acquire. Assets represent physical products with unique identifiers such as a serial number, a configuration, or a contact. You define assets that are based on a model and the information specific to the asset is added to the asset record. Define an asset record when you want to track cost, legal, and other ownership purposes of an asset.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Note: The search results only include assets that CA APM manages. If your repository contains assets that the product does not manage, those assets do not appear in the asset search results.

You can assign one lifecycle status to an asset to indicate its availability. If your administrator configured the asset search to include the Lifecycle Status field, you can retrieve information about assets based on the status.

Best Practices for Tracking Assets

When you manage assets, we recommend the following best practices:

- Enter useful information for cost, productivity, and decision making.
- If you cannot think of an immediate need, reconsider tracking the information.
- Keep the information accurate and up-to-date. If the information becomes outdated and obsolete, you do not know what information to trust. As a result, you can make incorrect purchasing and business decisions.
- Track expensive products and key components (such as system units, mainframes, large devices, printers, and monitors) as assets. Do not maintain information about IT assets that are not important when making purchasing and business decisions.
- Track a product as an asset only if you want to know the detailed information (such as the cost, serial number, bar code number, location) about each instance of that product. For example, if you want to know the location of each monitor of a particular model being used, or the cost of each monitor of a model.
- If you are using a discovery product to track the usage of hardware or software products, consider the following information:
  - The discovery product, instead of CA APM, tracks the product types.
  - The product types that the discovery product and CA APM must track support a comparison of usage and ownership information.

Asset Families

You can classify assets and models that are based on an asset family. An *asset family* is a way to organize and classify assets to track specialized information about products, services, or equipment that you use. The asset family determines the information that you see on the page when you enter an asset.

The product provides a set of predefined asset families, such as computer, hardware, other, projects, service, and software. Your administrator can create user-defined asset families based on the internal structure of your organization. When you define an asset, select either a predefined asset family or a user-defined asset family.

For each asset family, you can create a hierarchy to track an asset to a precise location. Assets inherit the asset family from the model records on which they are based.

Asset Classification

Asset classification helps reduce the number of records that are returned in searches and reports. When you define a model and asset, you can classify the objects by asset family. You can further classify models and assets in the following ways:

- **Class**. Broadly categorizes the product, such as a printer.
- **Subclass**. Provides additional refinement, such as inkjet or laser printer.

Assets inherit class and subclass assignments from the models on which they are based. Consider the following information when classifying assets:

- If you change the class and subclass for a model, the change is not automatically made to saved assets based on the model. The changes are not retroactive.
- You can change the class or subclass that an asset inherits from the model.

Manage Assets

You can add information about each asset to the repository so that you can manage assets throughout their lifecycle. Assets are defined based on models, and inherit data from the selected model. For example, you have defined Dell Precision Workstation 410 as a model. Your enterprise has purchased 100 individual computers, and you define 100 asset records that are based on the model to describe the individual computers.

Follow these steps:

1. Click Asset and perform one of the following actions.
2. **Define an asset.**
   a. Click New Asset.
   b. Enter the asset information.
   c. Associate the asset with other objects such as contacts, organizations, and companies.

      Associating assets with other objects enables data access to roles or users when you implement multi-tenancy.

   Note: You can also define an asset by copying an existing asset, supplying a new name, changing the asset information, and saving the new asset.
3. **Update an asset.**
   a. Search for the list of available assets.
   b. Click the asset that you want to update.
   c. Enter the new information for the asset.

   Note: You can also view and edit an object that is related to your asset, if the related object has a Browse icon. When you click the Browse icon, you leave the asset page and you navigate to the related object page. To keep the asset page in view and preserve the asset information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished.
4. **Delete an asset.**
   a. Search for the list of available assets.
   b. Click the asset that you want to delete.
   c. Click Delete and confirm that you want to delete the asset.

   Note: If the CI check box is selected (on the Asset Details page) for the asset you want to delete, you cannot delete the asset. The selected CI check box indicates that CA Service Desk Manager manages the asset. Delete the asset from CA Service Desk Manager.

   Important! We do not recommend that you delete an asset because the audit history for the asset is permanently removed. For example, legal, cost, relationship, and other information that is related to the asset is also deleted. Instead, update the asset status to indicate that the asset has been disposed of, or is *obsolete*. Using this approach, you retain the information about the asset in your repository for future reporting and reference purposes.
5. Click Save.

Add an Asset that CA CMDB Manages

You can add assets to your repository that CA CMDB manages. CA CMDB is integrated with CA Service Desk Manager. After you add an asset that CA CMDB manages, you can then open CA Service Desk Manager from CA APM and view and manage the asset.

Note: You can also create a configuration item (CI) in CA CMDB and then view it as an asset in CA APM. For more information about creating a configuration item, see the *CA Service Desk Manager Administration Guide*.

Important! You cannot delete an asset in CA APM that CA CMDB manages. You can only delete assets in CA APM that CA APM manages.

Follow these steps:

1. Click Asset, New Asset.
2. Enter the asset information.
3. Select the CI check box to have CA CMDB and CA Service Desk Manager manage the asset.

   Important! After you save an asset with the CI check box selected, you cannot update the asset to clear the CI check box.
4. Associate the asset with other objects such as contacts, organizations, and companies. This approach enables specific data access to roles or users when you implement multi-tenancy.
5. Click Save.
6. (Optional) View the new asset in CA Service Desk Manager by clicking the CA CMDB hyperlink at the top of the page.
7. Log in to CA Service Desk Manager.

   A CA Service Desk Manager window opens and the details of the selected asset appear.

Associate a Legal Document with an Asset

You associate assets and legal documents to identify the assets that a legal document covers. For example, you associate a volume purchase agreement with 100 laptops. Initiate this association from either the legal document or asset. You can associate multiple assets to a single legal document and multiple legal documents to a single asset.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the asset that you want to associate with a legal document.
4. Expand Relationships (on the left) and click Legal Documents.
5. Click Select New in the Legal Document section, search for and select a legal document.
6. Click Save.

Add and Remove Asset Legal Document Terms and Conditions

Terms and conditions are specific areas of agreement that are defined in legal documents. For example, legal documents can have terms and conditions for a multiproduct discount, a new pricing model, or copyright protection. After you associate a legal document with an asset, add or remove terms and conditions for the asset legal document from the Asset or Legal Document (see page 95) page.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to add or remove legal document terms and conditions.
4. Expand Relationships (on the left) and click Legal Documents.
5. Click the Edit Record icon for the legal document for which you want to add or remove terms and conditions.
6. Click View Assigned T's & C's.

7. Select one of the following options:
   - Click Select New for the date-specific or non-date-specific terms and conditions to add to the asset legal document.
   - Click the Mark for Deletion icon for the terms and conditions that you want to remove from the asset legal document.
8. Click Save.

Change an Asset Model

You can change the model for selected assets. For example, you identified 15 assets that were entered into the product with an incorrect server model. You search for the assets and select them. You then can change the server model for all selected assets simultaneously.

Follow these steps:

1. Click Asset.
2. Click Change Asset Model under Mass Change Utilities on the left.
3. Select the original model and the new model and click Go.

   All assets that have the original model are listed in the Search results. If you do not select an original model, all assets that do not have models are listed.

   Note: If the original model asset family has extended fields that the new model asset family does not have, a warning message appears. If you proceed with changing the asset model, the extended fields are lost. To avoid the data loss, define the extended fields for the new model asset family before you change the asset model.
4. (Optional) Select Assign Model Class to All Assets if you want all the listed assets to use the new model class.

   Note: This check box is available only if the new model has a class.
5. Select the individual assets that you want to change or select all assets.
6. Click Change Model.

   Your request is submitted.
7. Click View Mass Change Utilities Progress to see the status of your job.

View an Asset in CA Service Desk Manager

When you integrate the product with CA Service Desk Manager, you can select an asset in CA APM and view the asset information in CA Service Desk Manager.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset that you want to view in CA Service Desk Manager.
4. Click the CA CMDB hyperlink at the top of the page.

   Note: You can see the CA CMDB hyperlink only if the product is integrated with CA Service Desk Manager and if your user role includes asset configuration privileges.
5. Log in to CA Service Desk Manager.

   A CA Service Desk Manager window opens and the details of the selected asset appear.

   Note: Asset information that you enter in the product is not immediately available in CA Service Desk Manager. By default, a 10-minute delay exists from the time an asset is updated and the time you can view the asset in CA Service Desk Manager. For more information about the CA APM integration with CA Service Desk Manager, see the *CA Service Desk Manager Administration Guide*.

View Discovered and Owned Information for an Asset

You can view the discovered information for the owned assets that are linked with discovered assets during hardware reconciliation. Discovered information for an asset includes system configuration, operating system, system devices, file systems, and other information. You can also view the owned information for the assets that you define in the product. Owned information for an asset includes asset properties (for example, operating system and product version), legal information, installed software, components, and other information.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.

3. Click the asset for which you want to view the information and perform one of the following steps:

   - Click Discovered Information.

     Note: The Discovered Information hyperlink appears only for assets that are reconciled.

   - Click Owned Information.

     Note: If the product is integrated with CA Service Desk Manager, CA Client Automation, and CA SAM, you can see the asset information from those products.

   An asset viewer window opens and displays the information. The links on the window let you access more details.

4. Click each link to view the specific information.
5. Close the window when you are finished viewing the information.

Hardware Assets

CA APM lets you track the hardware asset information that your company is entitled to use. For each hardware asset, you can track the following information:

- Maintain a record of cost and legal information.
- Maintain a record of components in asset configuration and the configurations where the asset is a component.
- Maintain the availability status of the asset.
- Track the software details that are allocated to the asset.

Add Components in an Asset Configuration

An asset can inherit the components from a model. CA APM lets you add components to an asset configuration, for example, an external hard drive or a DVD writer.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to add components.
4. Expand Configurations on the left and click Asset Configuration.
5. Click Select New in the Asset Configuration section, search for and select an asset.
6. Click Save.

Update the Asset Status

CA APM lets you change the lifecycle status of an asset. For example, you can update the status when the asset changes from received to available.

To update the asset status

1. Click Asset.
2. Search to find the list of available assets.
3. Click the asset for which you want to update the status.
4. Change the Lifecycle Status and Lifecycle Status Date fields to the appropriate status and date for the asset.
5. Click Save.

   The status for the asset is updated.

Track Image Partitions

CA APM lets you enter image partition details for an existing asset and track them. For example, you can specify that the hard disk on a computer has two partitions and enter the size in GB for each partition. Create an image partition as a separate asset and associate it with the parent asset.

Note: You can view an audit history for this relationship.

To track image partition details

1. Click Asset.
2. Search to find the list of available assets.
3. Click the asset for which you want to enter image partition details.
4. On the left, expand Relationships and click Image Partitions.
5. Click Select New and select a different asset, other than the asset previously selected.
6. Click Save.

   The image partition details are saved and can be tracked.

Asset Groups

An *asset group* is a collection of assets that you acquire together and that are based on the same model. You define an asset group in one asset record. The value in the Quantity field on the Asset Details page indicates the number of assets in the group. The product tracks the asset information for the entire group, rather than for the individual assets. All members of an asset group share asset information.

Asset groups are useful in the following situations:

- The assets are covered under the same purchase or license agreement. You do not need to track cost, payment, licensing, and legal information separately for each asset.
- The assets share some common information, but some of the individual assets in the group have different information. In this situation, you first define the assets as a group and enter the common information one time. Then, you divide the asset group into individual assets (subgroup the asset group) and enter any information that is unique to the individual assets.

You do not have to use asset groups when you are billed for assets on a single invoice. You can record payments for assets that are tracked separately, regardless of whether they were billed on the same invoice.

Asset Subgrouping

CA APM lets you divide (subgroup) an asset group into individual assets using the product. When you subgroup assets, the data for the asset group is copied to the new individual assets, *except* for the following information:

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

You can change any existing data or add unique information to the new individual assets. You track the new assets separately from that point forward.

Example: Subgroup Software Licenses

In this example, you purchase 100 licenses of Microsoft Visual Studio under a single purchasing agreement. You record the licenses as an asset group with a quantity of 100. Later, you allocate ten licenses to members of your development staff. You then subgroup the ten allocated licenses into individual assets and enter their allocation information. The 90 licenses that are not allocated remain in the asset group.

Define an Asset Group

CA APM lets you add information to the repository about a group of assets that share common information. You can then manage these assets as a group throughout their lifecycle. You can divide (subgroup) the asset group into individual assets later so that you can specify and track unique information for the individual assets.

Follow these steps:

1. Click Asset, New Asset.
2. Enter the asset information.
3. In the Quantity field, enter the total number of assets in the group. You enter a value greater than one for an asset group.
4. Associate the asset group with other objects such as contacts, organizations, and companies. This approach enables specific data access to roles or users when you implement multi-tenancy.
5. Click Save.

Subgroup an Asset Group

CA APM lets you divide an asset group into individual assets when you want to manage assets in the group separately. When you subgroup an asset group, the product removes assets from the group (decreases the group quantity) and creates either one new asset or multiple new assets (depending on your criteria). The product copies the information for the group to the new assets, except Serial Number, Alt Asset ID, Host Name, DNS Name, and MAC Address.

Follow these steps:

1. Click Asset.
2. Search to find the list of available assets.
3. Click the asset that you want to subgroup.

   The Asset Details page for the selected asset appears.
4. Click Subgroup.

   Note: The Subgroup button is enabled only for an asset with a quantity greater than one.

   The Subgroup Asset wizard appears.

5. Select a subgrouping option and click Next. The following fields require explanation:

   Create a new asset

   Divides the original asset group into two assets. You specify the quantity for the new asset. The remaining quantity is left with the original asset.

   For example, you have an asset group with a quantity of 50. You want to divide the group into two assets with a quantity of 35 for the new asset and 15 for the original asset. You use this subgrouping option and specify 35 for the new asset quantity.

   Create individual assets each with a quantity of one

   Divides the entire quantity of the original asset group into multiple assets. Each asset has a quantity of one.

   For example, you have an asset group with a quantity of 25. You want to divide the group into 25 individual assets. You use this option.

6. Follow the wizard to define unique asset names and to specify the data that you want to copy to the new assets.

   Note: If you do not define unique asset names, the new assets retain the name of the original asset group.

7. Click Finish when you have completed the wizard.

8. Click Save.

Asset Registration

Use the *asset registration process* to report on a single asset and identify the instances of the asset within all asset functional areas through asset registration fields. These fields help ensure that assets within an asset functional area are not duplicated.

The following fields on the Asset Details page represent the asset registration fields:

- Asset Name
- Serial Number
- Asset Tag (represented on the page as Alt Asset ID)
- Host Name
- DNS Name
- MAC Address

Asset Configurations

An *asset configuration* is a description of an asset (for example, a desktop computer) and its individual components (for example, personal productivity software, monitor, modem, and so forth). CA APM lets you track the configuration information for both an asset and model. In addition, you can associate an asset or model record to their component asset and model records to initiate a relationship between them.

This information helps you maintain historical information about the changes to a configuration for an asset over the course of its life. You can define configuration records for any model or asset in the repository.

Asset configuration records can be of the following types:

- **Model configuration**. Describes the configurations that manufacturers currently offer and any substitutions or additions that your company typically makes to those configurations when you purchase them. Use this type of configuration record to describe configurations for hardware models.
- **Asset configuration**. Describes the configurations of existing hardware assets. Use this type of configuration record when the asset configurations are different from the standard model configurations to indicate the changes between the model and asset configurations. You can also use this configuration type to describe changes to existing configurations.

You can change these configuration types at any time and manage the changes.

More information:

Add Components in a Model Configuration (see page 27)
Add Components in an Asset Configuration (see page 35)

Add Components in a Model Configuration

You associate a hardware model to its component models to define a model configuration. A generic model is a model that is not acquired as an asset, for example, keyboards and network cards. Generic models comprise a model configuration. This configuration is available to the inherited assets from the model.

Follow these steps:

1. Click Model and search for the list of available models.
2. Click the model for which you want to add components.
3. Expand Configurations on the left and click Model Configuration.

4. Click Select New, search for and select a model.
5. Click the Edit Record icon next to the model name to define the association between the hardware model and model components.
6. Click Save.

Define Generic Model Configuration Details

CA APM lets you define configuration details for a generic model on which an asset can be based.

Follow these steps:

1. Click Model.
2. Search for the list of available models.
3. Click the model for which you want to define a generic configuration.
4. Expand Configurations on the left and click Model Configuration.
5. Click Select New to search for and select a model.
6. Click Save.

Define Generic Asset Configuration Details

CA APM lets you define configuration details for a generic asset.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to define a generic configuration.
4. Expand Configurations on the left and click Model Configuration.
5. Click Select New to search for and select a model.
6. Click Save.

Define Specific Asset Configuration Details

CA APM lets you define a specific asset configuration.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to define a specific configuration.
4. Expand Configurations on the left and click Asset Configuration.
5. Click Select New to search for and select an asset.
6. Click Save.

Add Components in an Asset Configuration

An asset can inherit the components from a model. CA APM lets you add components to an asset configuration, for example, an external hard drive or a DVD writer.

Follow these steps:

1. Click Asset.
2. Search for the list of available assets.
3. Click the asset for which you want to add components.
4. Expand Configurations on the left and click Asset Configuration.
5. Click Select New in the Asset Configuration section, search for and select an asset.
6. Click Save.

Update or Delete a Configuration Record

CA APM lets you update or delete a configuration record.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Model or Asset.
2. Search for the model or asset for which you want to update or delete the configuration record.

3. Click the model or asset in the search results list.
4. Expand Configurations on the left and click the appropriate configuration option. For example, click Asset Configuration or Model Configuration.
5. Perform the steps for one of the following actions.
6. Update the configuration record.
   a. Click the Edit Record icon next to the configuration record.
   b. Select the new information for the configuration record.
   c. Click Save.
7. Delete the configuration record.
   a. Click the Mark for Deletion icon next to the configuration record.
   b. Click Save.

View the Configuration When an Asset is a Component

CA APM lets you view the configuration when an asset is a component.

Follow these steps:

1. Click Asset.
2. Search for the asset for which you want to view the configuration.
3. Click the asset in the search results list.
4. Expand Configurations on the left and click Asset Configuration.

   The list of assets in the specific configuration appears.

Costs and Payments

CA APM lets you track financial information that is associated with assets and legal documents. Tracking costs and payments helps reduce the risk of overpaying or underpaying vendors and suppliers. This information is also useful when deciding about future equipment purchases and deployment.

In addition to tracking cost-related information for assets and legal documents, use cost records with payments to create *payment schedules.* The schedules can help you make timely payments and reduce the risk of overpayment. The information that you provide on the Cost page is used to calculate the payment schedules. If you define the cost as a recurring cost, the schedule includes multiple payment records. For example, if you enter a cost that recurs monthly for one year, the product automatically creates 12 payment records. If the cost is a one-time cost (not a recurring cost), the schedule includes only a single payment record.

Cost records store information about costs and billing, payees, recurring charges, and one time charges. Payment records maintain information about individual payments that are related to a specific cost. A payment record also calculates and displays the total scheduled payment amount, total paid amount, and the balance due for a given cost. A payment record can represent a single payment of the full cost or multiple partial payments.

Define the Parts and Pricing for a Model

You can define the parts and pricing details for a model to identify the individual component costs that comprise the total cost for a model. For example, you have a model named Dell Precision Workstation 410. You can define the parts and pricing for the internal drives, video connectors, USB connectors, SCSI port connectors, and power supply.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Model.
2. Search to find the list of available models.
3. Click the model for which you want to define the parts and pricing.
4. In the Parts and Pricing area of the page, click New and enter the parts and pricing details.
5. Click Save.

Define the Cost for an Asset or Legal Document

Defining asset costs helps you track and manage the financial information that is related to a specific asset or legal document. You can add multiple cost records for an asset or legal document. You can also add cost information to multiple assets or legal documents and update multiple payment records.

Follow these steps:

1. Click Asset or Legal Document.
2. Search to find the list of available items.
3. Click the asset or legal document that you want to update.
4. On the left, click Costs.

5. Click New and enter the cost information.

   The following fields require explanation:

   Unit Amount

   Specifies the cost per unit.

   Total Amount

   Displays the total cost for the total quantity of the selected asset. This amount is calculated automatically by multiplying the Unit Amount on the Costs page by the Quantity on the Asset Details page.

   Recurring Period

   Specifies the number of Recurring Period Units (days, months, or years) after which the cost recurs. For example, if you enter 1 for the Recurring Period and select Month for the Recurring Period Units, the cost recurs every month.

   Note: If you specify a value other than zero, select the Recurring Period Units and Termination Date.

   Recurring Period Units

   Specifies the unit (days, months, or years) for the Recurring Period.

   Termination Date

   Specifies the last date for the recurring schedule.

6. Click Save.

   Note: If you specify recurring period information for an asset cost, a payment schedule with multiple payments is automatically created. If you do not specify recurring period information, the payment schedule includes only one payment.

7. (Optional) View the payment schedule for the cost that you defined using the following steps:

   a. Click the Edit Record icon for the cost record.

   b. Click Show Payments on the right.

      Note: You can record payments that you made for this cost.

Delete a Cost Record

You can delete the cost record of an asset or legal document. The payment records that are associated with the deleted cost record are also deleted.

Important! When you delete a cost record, you can no longer view the audit history for the record.

Follow these steps:

1. Click Asset or Legal Document.
2. Search for and select the asset or legal document for which you want to delete the cost record.
3. On the left, click Costs.
4. Click the Mark for Deletion icon for the records you want to delete.

   Note: To reverse the Mark for Deletion selection, click the Undo Record Deletion icon.
5. Click Save.

More information:

Define the Cost for an Asset or Legal Document (see page 44)

Events and Notifications

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.

Escalation of Notifications

When an event occurs, the workflow provider sends an email notification to the recipients that you specified when you defined the event. CA APM lets you send email notifications to different levels of recipients.

- *Initial recipients* are the primary recipients of the notification. They are the first users to receive the notification and to respond and acknowledge the notification. The notification contains information about the event that you specified when you defined the event. The recipient receives a reminder email before the acknowledgment due date arrives. If the recipient still does not acknowledge the notification by the due date, the notification is escalated if you selected a workflow process with escalation.

- *Escalation recipients* are secondary recipients of the notification. If the initial recipients do not acknowledge the notification within a specified time frame, the product escalates the notification to the escalation recipients if you selected a workflow process with escalation. Escalations help ensure that someone is notified about an important date or event when the initial recipient is not available to acknowledge the notification. The product includes the following workflow processes and escalations:
  - Notification and One Escalation–Sends a notification to the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.
  - Notification without ACK–Sends a notification to the initial recipient and marks the event as completed. The recipient does not need to respond and the process does not escalate the notification.
  - Notification without Escalation–Sends a notification to the initial recipient and sends a reminder email. If the recipient does not respond, the process marks the event as failed. If the recipient responds in the specified time frame, the process marks the event as completed.

The notification levels let you notify one or more users about an event and provide separate instructions to each user. You define the recipients and the notification escalation levels when you specify the workflow provider process parameters (see page 65) for an event.

Acknowledgements

An email notification is acknowledged when the recipient opens the email, clicks the link to CA Process Automation, logs in to CA Process Automation, and acknowledges receipt of the notification. You acknowledge an email notification in the workflow provider.

The email that is sent to the initial recipient contains the message that you specified when you defined the event. If a user does not acknowledge receipt of the email, the notification is escalated to the next responsible recipient if the selected workflow process includes escalations. When a notification is acknowledged, the product does not perform any future escalations for the same event notification.

Email Notification Process Selection

When a date, change, or watch event occurs, the email notification process is started in the workflow provider (for example, CA Process Automation). You define and set up the email notification process in the workflow provider and in CA APM (for example, you define the email recipients, levels of escalation, and notification text). CA APM lets you define different types of notification processes in the workflow provider. For example, you can have an email notification process (provided with the product) and another user-defined process that initiates actions in an external application, such as an asset management dashboard. You select the notification process that you want to use with a specific event when you define the event.

Note: For more information about defining notification processes in the workflow provider, see your workflow provider documentation.

The type of email notification process that is started after an event occurs depends on the process that you selected when you defined the event. The following email notification processes are provided with the product and apply to the CA Process Automation workflow provider:

- Notification and One Escalation–Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.
- Notification without ACK–Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.
- Notification without Escalation–Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time frame, the process marks the event as failed. If the recipient acknowledges within the specified time frame, the process marks the event as completed.

You can define additional notification processes in the workflow provider that perform other actions (in addition to email notifications) when events occur. You can then select one of your own defined processes when you define an event.

How to Manage 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 manage events and notifications, complete the following steps:

1. Administrators grant permissions to users to manage events.

   Note: For more information about the permissions to manage events, see the *Administration Guide*.

2. Open an existing local or global configuration and define any of the following events:

   - Date event (see page 50)
   - Change event (see page 55)
   - Watch event (see page 59)

3. When defining an event, map all required workflow provider notification parameters to a CA APM object attribute (see page 65).
4. The workflow provider initiates the email notification process.
5. View an audit history of events (see page 119).
6. (Optional) The notification recipient acknowledges the notification (see page 48).

Date Events

Use a *date event* to monitor a date field for an object and have the workflow provider (for example, CA Process Automation) notify you that an important date is approaching or has passed. Date events are based on the value that is stored in a specific date field (default and extended fields), and the notification from the workflow provider provides an advanced warning to alert someone to complete a follow-up task. The date on which a user is notified about the upcoming or passed event is based on the field value for the object and the information that you specify when you define the event, including the Days After value (see page 51).

CA APM lets you define one or more date events for a single field.

Note: As a rule, events are not triggered (and notifications are not sent) for field changes that happened before the event was defined. An exception to this rule occurs for date events. If the notification date occurs *after* the event was defined, an event is triggered (and a notification is sent) even if the field change happened *before* the event was defined.

Example: Define a Date Event to Terminate a Legal Document

In this example, a contract negotiator must review contracts thirty days before they expire. You define a date event on the Terminate Date field for a legal document. For example, when the contract manager adds a legal document for which the termination date is 3/31/2010, a notification is sent to the appropriate person on 3/1/2010.

Define a Date Event

CA APM lets you define a date event to monitor a date field and have the workflow provider (for example, CA Process Automation) notify you that an important date is approaching or has passed. For example, you can define a date event on the Terminate Date field for a legal document. You can define one or more date events for a single field.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To define a date event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.
5. Click New.
6. Specify the information for the date event.

   The following fields require explanation:

   Event Type

   Select the type of event as a date event. After you select the event type and save the event, you cannot change the event type. If you select the incorrect event type when defining an event, delete the event and define it again using the correct event type.

Days After

Specify a positive or negative number to indicate how many days before or after a field change occurs to create a date event.

- A positive number indicates how many days after the original value has passed to create a date event.
- A negative number indicates how many days before the original value approaches to create a date event.

Inactive

Select this check box to indicate that the date event is inactive. When you make a date event inactive, no new notifications are created for the event. However, pending notifications are processed.

Event Provider

Select the workflow provider to notify users that the date event has occurred (for example, CA IT Process Automation Manager). When you select a provider, all available workflow processes for the selected provider appear in the Workflow Process field.

Workflow Process

Identifies the workflow process for the workflow provider. When you select a workflow process, all available process parameters for the workflow provider appear.

- Notification and One Escalation–Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.
- Notification without ACK–Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.
- Notification without Escalation–Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time period, the process marks the event as failed. If the recipient acknowledges within the specified time period, the process marks the event as completed.
- (Optional) Additional Process Types–Uses processes you defined in the workflow provider.

Notification Parameters

Specify each process parameter for the workflow provider by doing one of the following in each field:

- Enter an actual (hard-coded) value.
- Click Map Fields to map the parameter to a CA APM object attribute (see page 65).
- Enter an actual (hard-coded) value and, in the same field, click Map Fields to map the parameter.

Note: Refer to the field tooltips for specific information about the format and content of each parameter field.

7. Click Save.
8. Click CONFIGURE: OFF.

   The configuration of the date event is complete.

Update a Date Event

CA APM lets you update the information for an existing date event. For example, you can change the event name and description, and you can make the event inactive.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To update a date event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.
5. Click the Edit Record icon next to the date event that you want to update.
6. Enter the new information for the date event.

   Note: After you define and save an event, you cannot change the Event Type, Event Cause, Value Changed From, and Value Changed To. If you enter the incorrect information, delete the event and define it again using the correct information.

7. Click the Complete Record Edit icon.
8. Click Save.
9. Click CONFIGURE: OFF.

   The configuration of the date event is complete.

Delete a Date Event

CA APM lets you delete a date event that you do not need. For example, when you do not want to be notified about a change to the Terminate Date field for a legal document, you can delete the associated date event. If your administrator has granted you the correct permissions, you can complete this task.

Note: Any pending notifications from the workflow provider (for example, CA Process Automation) about the event are sent before the event is deleted. When you delete an event, all historical information about the event is deleted. We recommend that instead of deleting the event, you make the event inactive (see page 75). That way, if you need the event in the future, you do not have to redefine it.

To delete a date event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.
5. Click the Mark for Deletion icon next to the date event that you want to delete.
6. Click Save.
7. Click CONFIGURE: OFF.

   The configuration of the date event is complete.

Change Events

Use a *change event* to monitor a field for an object and have the workflow provider (for example, CA Process Automation) notify you that the field value has changed. Change events are based on the value that is stored in a specific field (default and extended fields), and the notification from the workflow provider provides a warning to alert someone when the value of a field is set or changes.

CA APM lets you define one or more change events for a single field.

Example: Define a Change Event to Find Equipment for a New Employee

In this example, asset technicians provide the appropriate equipment when an employee is hired or transferred to a different department. You define a change event that issues a notification to a member of the asset technician team when the Department field value for the contact is set or changes. This notification alerts the technician to find equipment for the new or transferred employee.

Define a Change Event

CA APM lets you define a change event to monitor a field and have the workflow provider (for example, CA Process Automation) notify you that the field value has changed. For example, you can define a change event on the Department field for a contact. You can define one or more change events for a single field.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To define a change event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.

5. Click New.
6. Specify the information for the change event.

   The following fields require explanation:

   Event Type

   Select the type of event as a change event. After you select the event type and save the event, you cannot change the event type. If you select the incorrect event type when defining an event, delete the event and define it again using the correct event type.

   Event Cause

   Select the type of action that must happen to the field for the change event to occur. Supported event causes include when a field is changed, a record is added, and a record is deleted.

   Value Changed From

   Select the initial state of the field value for the change event to occur. Supported field value changes include the following options:

   - **Any value**. Any field value sets the initial state.
   - **Blank**. A blank field value sets the initial state.
   - **Old value**. A specific value sets the initial state.

   Value

   Available when you select *Old value* in the Value Changed From field. Enter a specific value to set the initial state.

   Value Changed To

   Select the final state of the field value for the change event to occur. Supported field value changes include the following options:

   - **Any value**. Any field value, except a blank value, sets the final state.
   - **Blank**. A blank field value sets the final state.
   - **New value**. A specific value sets the final state.

   Value

   Available when you select *New value* in the Value Changed To field. Enter a specific value to set the final state.

   Inactive

   Select this check box to indicate that the change event is inactive. When you make a change event inactive, no new notifications are created for the event. However, pending notifications are processed.

Event Provider

Select the workflow provider to notify users that the change event has occurred (for example, CA IT Process Automation Manager). When you select a provider, all available workflow processes for the selected provider appear in the Workflow Process field.

Workflow Process

Identifies the workflow process for the workflow provider. When you select a workflow process, all available process parameters for the workflow provider appear.

- Notification and One Escalation–Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.
- Notification without ACK–Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.
- Notification without Escalation–Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time period, the process marks the event as failed. If the recipient acknowledges within the specified time period, the process marks the event as completed.
- (Optional) Additional Process Types–Uses processes you defined in the workflow provider.

Notification Parameters

Specify each process parameter for the workflow provider by doing one of the following in each field:

- Enter an actual (hard-coded) value.
- Click Map Fields to map the parameter to a CA APM object attribute (see page 65).
- Enter an actual (hard-coded) value and, in the same field, click Map Fields to map the parameter.

Note: Refer to the field tooltips for specific information about the format and content of each parameter field.

7. Click Save.
8. Click CONFIGURE: OFF.

The configuration of the event is complete.

Update a Change Event

CA APM lets you update the information for an existing change event. For example, you can change the event name and description, and you can make the event inactive.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To update a change event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.
5. Click the Edit Record icon next to the change event that you want to update.
6. Enter the new information for the change event.

   Note: After you define and save an event, you cannot change the Event Type, Event Cause, Value Changed From, and Value Changed To. If you enter the incorrect information, delete the event and define it again using the correct information.
7. Click the Complete Record Edit icon.
8. Click Save.
9. Click CONFIGURE: OFF.

   The configuration of the change event is complete.

Delete a Change Event

CA APM lets you delete a change event that you do not need. For example, when you do not want to be notified about a change to the Department field for a contact, you can delete the associated change event. If your administrator has granted you the correct permissions, you can complete this task.

Note: Any pending notifications from the workflow provider (for example, CA Process Automation) about the event are sent before the event is deleted. When you delete an event, all historical information about the event is deleted. We recommend that instead of deleting the event, you make the event inactive (see page 75). That way, if you need the event in the future, you do not have to redefine it.

To delete a change event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.
5. Click the Mark for Deletion icon next to the change event that you want to delete.
6. Click Save.
7. Click CONFIGURE: OFF.

   The configuration of the change event is complete.

Watch Events

Use a *watch event* to monitor a field for an object and have the workflow provider (for example, CA Process Automation) notify you about a potential obstruction to completing a task. Watch events are based on inactivity on a particular field (default and extended fields) within a specified time period, and the notification from the workflow provider provides an advanced warning to alert someone about a potential obstruction. If the field value changes within the time period, the workflow provider does not send a notification.

CA APM lets you define one or more watch events for a single field.

Example: Define a Watch Event to Configure and Deploy New Laptops

In this example, you require that asset technicians configure and deploy all new laptops to employees within five days of receiving the laptop. To meet this requirement, you define a watch event that creates an event when an asset is assigned a status (Lifecycle Status field) of received. If the status remains received for more than five days, a notification is sent to an asset technician.

Define a Watch Event

CA APM lets you define a watch event to monitor a field and have the workflow provider (for example, CA Process Automation) notify you about inactivity on a particular field. For example, you can define a watch event on the Lifecycle Status field for an asset. You can define one or more watch events for a single field.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To define a watch event

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.

5. Click New.
6. Specify the information for the watch event.

   Important! The Value Changed From and Value fields work together to start the timer for the watch event. The timer continues for the duration that you specify in the Days After field. The Value Changed To and Value fields work together to indicate the value that you want to achieve and stop the timer. If the value that you want to achieve does not occur in the specified time period after the timer starts, the watch event occurs and indicates that the defined workflow did not happen.

   The following fields require explanation:

   Event Type

   Select the type of event as a watch event. After you select the event type and save the event, you cannot change the event type. If you select the incorrect event type when defining an event, delete the event and define it again using the correct event type.

   Event Cause

   Select the type of action that must happen to the field for the watch event to occur. A supported event cause is when a field is changed.

   Days After

   Specify a positive number to indicate how many days to wait after the Value Changed From field value to start the watch timer.

   Note: If the Value Change To field value does not occur, the watch timer expires after the number of days that you specify. After the watch timer expires, the watch event is created. However, the watch timer will stop when the Value Change To field value changes to the specified value and no watch event is created.

   Value Changed From

   Select the initial field value to start the timer to create the watch event. Supported field value changes include the following options:

   - **Any value**. Any field value starts the timer for the watch event.
   - **Blank**. A blank field value starts the timer for the watch event.
   - **Old value**. A specific initial value starts the timer for the watch event.

   Value

   Available when you select *Old value* in the Value Changed From field. Enter a specific value to start the timer for the watch event.

Value Changed To

Select the final state of the field value that stops the timer for the watch event and prevents the watch event from occurring. Supported field value changes include the following options:

- **Any value**. Any field value stops the timer for the watch event and prevents the watch event from occurring.
- **Blank**. A blank field value stops the timer for the watch event and prevents the watch event from occurring.
- **New value**. A specific field value stops the timer for the watch event and prevents the watch event from occurring.

Value

Available when you select *New value* in the Value Changed To field. Enter a specific value to stop the timer for the watch event and prevent the watch event from occurring.

Inactive

Select this check box to indicate that the watch event is inactive. When you make a watch event inactive, no new notifications are created for the event. However, pending notifications are processed.

Event Provider

Select the workflow provider to notify users that the watch event has occurred (for example, CA IT Process Automation Manager). When you select a provider, all available workflow processes for the selected provider appear in the Workflow Process field.

Workflow Process

Identifies the workflow process for the workflow provider. When you select a workflow process, all available process parameters for the workflow provider appear.

- Notification and One Escalation–Notifies the initial recipient and sends a reminder email. If the recipient acknowledges the notification, the process marks the event as completed. If the recipient does not acknowledge in the specified time frame, the process escalates the notification to the escalation recipient. If the escalation recipient responds, the process marks the event as completed. If the escalation recipient does not respond, the process marks the event as failed.
- Notification without ACK–Notifies the initial recipient and marks the event as completed. The recipient does not need to acknowledge the notification.

- Notification without Escalation–Notifies the initial recipient and sends a reminder email. If the recipient does not acknowledge the notification within the specified time period, the process marks the event as failed. If the recipient acknowledges within the specified time period, the process marks the event as completed.
- (Optional) Additional Process Types–Uses processes you defined in the workflow provider.

Notification Parameters

Specify each process parameter for the workflow provider by doing one of the following in each field:

- Enter an actual (hard-coded) value.
- Click Map Fields to map the parameter to a CA APM object attribute (see page 65).
- Enter an actual (hard-coded) value and, in the same field, click Map Fields to map the parameter.

Note: Refer to the field tooltips for specific information about the format and content of each parameter field.

7. Click Save.
8. Click CONFIGURE: OFF.

   The configuration of the watch event is complete.

Update a Watch Event

CA APM lets you update the information for an existing watch event. For example, you can change the event name and description, and you can make the event inactive.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To update a watch event

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

   The configuration of the event is enabled.

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

   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 Event Configuration icon.

   The Events page for the selected field appears.

5. Click the Edit Record icon next to the watch event that you want to update.

6. Enter the new information for the watch event.

   Note: After you define and save an event, you cannot change the Event Type, Event Cause, Value Changed From, and Value Changed To. If you enter the incorrect information, delete the event and define it again using the correct information.

7. Click the Complete Record Edit icon.

8. Click Save.

9. Click CONFIGURE: OFF.

   The configuration of the watch event is complete.

Delete a Watch Event

CA APM lets you delete a watch event that you do not need. For example, when you do not want to be notified about a change to the Lifecycle Status field for an asset, you can delete the associated watch event. If your administrator has granted you the correct permissions, you can complete this task.

Note: Any pending notifications from the workflow provider (for example, CA Process Automation) about the event are sent before the event is deleted. When you delete an event, all historical information about the event is deleted. We recommend that instead of deleting the event, you make the event inactive (see page 75). That way, if you need the event in the future, you do not have to redefine it.

To delete a watch event

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

2. On the left, click CONFIGURE: ON.

   The configuration of the event is enabled.

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

   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 Event Configuration icon.

   The Events page for the selected field appears.

5. Click the Mark for Deletion icon next to the watch event that you want to delete.

6. Click Save.

7. Click CONFIGURE: OFF.

   The configuration of the watch event is complete.

Workflow Provider Process Parameters

You perform some of the setup and configuration of the email notification process in the workflow provider. However, you also specify the process parameters for the workflow provider when you define an event in CA APM. The process parameters include items such as user IDs, email addresses, email subject, content of email, and other items. The workflow provider uses this information to construct, issue, and manage the email notification.

Note: For information about workflow provider process parameters that you must specify in CA Process Automation, see the *Implementation Guide.* For information about setting up a notification process, see your workflow provider documentation.

You can provide actual (hard-coded) values when you specify the process parameters. If you use an actual value for an email address (or another parameter), you must verify that the address (or other data) is valid.

You can also map the process parameters to CA APM object attributes. If you map a process parameter to a CA APM object attribute, the workflow provider accesses CA APM to find the current value of the mapped attribute and uses that value to construct and manage the notification. For example, you map the process parameter Initial Email Addresses to the CA APM attribute Contact Email Address when you define an event. When that event occurs, the workflow provider determines the current value of the CA APM Contact Email Address and uses that value for the Email ID.

Important! To map CA Process Automation process parameters to CA APM objects successfully, you must understand the CA APM data objects and the CA Process Automation parameters. You need to determine which CA APM object is an appropriate match for each CA Process Automation parameter.

Notification and One Escalation Process Parameters

The process parameters that appear when you define an event depend on the workflow provider process type that you select. The Notification and One Escalation process is an email notification process that is included with the product. This process sends an email notification to the initial recipient when an event occurs and, if the initial recipient does not respond, escalates the email to the first escalation level recipients. When you select this process as the workflow process for an event, a list of parameters appears.

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

The following fields require explanation:

Initial User IDs

CA Process Automation user ID (CA APM or non-CA APM user) for acknowledging the initial notification. You can specify more than one user ID, separated with colons. Do not enter spaces between entries.

Example: This example contains a user ID (John) that is a text entry value and the mapped field {legaldoc.owner.userid}. The two items are separated with a colon. The mapped field {legaldoc.owner.userid} represents the user ID of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.userid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select User ID from the list of attributes.

```
John:{legaldoc.owner.userid}
```

Initial Groups

CA Process Automation group name for acknowledging the initial notification. You can specify more than one group name, separated with colons. Do not enter spaces between entries.

Example: This example contains a CA Process Automation group name (ITAM) that is a text entry value.

```
ITAM
```

Initial Email Addresses

Email address (or distribution list) of the initial recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (john.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.owner.emailid} represents the email address of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select Email Address from the list of attributes.

```
john.doe@company.com;{legaldoc.owner.emailid}
```

Initial Email Copy Addresses

Email address (or distribution list) of the initial copy recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc.requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

Initial Email Subject

Subject of the email message for the initial recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Acknowledgement required for) and the mapped field {legaldoc.documentidentifier}.

```
Acknowledgment required for {legaldoc.documentidentifier}
```

Initial Email Message

Message of the email for the initial recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires
your acknowledgment using the link in the Subject of this email.
```

Acknowledgment Title

Title that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier) only.

```
The Legal Document Document Identifier
```

Acknowledgment Description

Description that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier) and the mapped field {legaldoc.documentidentifier}.

```
The Legal Document Document Identifier {legaldoc.documentidentifier}
```

Escalation User IDs

CA Process Automation user ID (CA APM or non-CA APM user) for acknowledging the escalation notification. You can specify more than one user ID, separated with colons. Do not enter spaces between entries.

Example: This example contains a user ID (Mary) that is a text entry value and the mapped field {legaldoc.owner.supervisor.userid}. The two items are separated with a colon. The mapped field {legaldoc.owner.supervisor.userid} represents the user ID of the supervisor of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.supervisor.userid}, click the Map Fields button, select the Owner link in the Add Fields dialog, select the Supervisor link, and select User ID from the list of attributes.

```
Mary:{legaldoc.owner.supervisor.userid}
```

Escalation Groups

CA Process Automation group name for acknowledging the escalation notification. You can specify more than one group name, separated with colons. Do not enter spaces between entries.

Example: This example contains a CA Process Automation group name (ITAM) that is a text entry value.

```
ITAM
```

Escalation Email Addresses

Email address (or distribution list) of the recipient of the escalation email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (mary.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.supervisor.emailid}. The two items are separated with a semicolon. To obtain the mapped field {legaldoc.owner.supervisor.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, select the Supervisor link, and select Email Address from the list of attributes.

```
mary.doe@company.com;{legaldoc.owner.supervisor.emailid}
```

Escalation Email Copy Addresses

Email address (or distribution list) of the copy recipients of the escalation email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc.requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

Escalation Email Subject

Subject of the escalation email. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Escalation for), the mapped field {legaldoc.documentidentifier}, and additional text entry content.

```
Escalation for {legaldoc.documentidentifier}. Acknowledgment required
```

Escalation Email Message

Message of the escalation email. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires
your acknowledgment using the link in the Subject of this email.
```

Reminder Email Subject

Subject of the reminder email message for initial and escalation recipients. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Reminder for), the mapped field {legaldoc.documentidentifier}, and additional text entry content.

```
Reminder for {legaldoc.documentidentifier}. Acknowledgment required.
```

Reminder Email Message

Message of the reminder email for initial and escalation recipients. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Reminder: The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
Reminder: The Legal Document Document Identifier {legaldoc.documentidentifier}
requires your acknowledgment using the link in the Subject of this email.
```

Acknowledgment Time-out (Days:Hours:Minutes)

The amount of time that is allowed for acknowledgment after the email notification is sent before the escalation process begins. This time-out applies to initial and escalation notifications. Days, hours, and minutes can be any numeric value. The format must be *days*:*hours*:*minutes* (separated with colons).

Example: This example specifies a time-out period of exactly four days.

```
4:00:00
```

Notification without ACK Process Parameters

The process parameters that appear when you define an event depend on the workflow provider process type that you select. The Notification without ACK process is an email notification process that is included with the product. This process sends an email notification to the specified recipient when an event occurs. The recipient does not need to acknowledge the notification, and the product does not escalate the notification. When you select this process as the workflow process for an event, a list of parameters appears.

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

The following fields require explanation:

Email Address

Email address (or distribution list) of the recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (john.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.owner.emailid} represents the email address of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select Email Address from the list of attributes.

```
john.doe@company.com;{legaldoc.owner.emailid}
```

Email Copy Address

Email address (or distribution list) of the copy recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc.requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

Email Subject

Subject of the email message for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Acknowledgment required for) and the mapped field {legaldoc.documentidentifier}.

```
Acknowledgment required for {legaldoc.documentidentifier}
```

Email Message

Message of the email for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires
your acknowledgment using the link in the Subject of this email.
```

Notification without Escalation Process Parameters

The process parameters that appear when you define an event depend on the workflow provider process type that you select. The Notification without Escalation process is an email notification process that is included with the product. This process sends an email notification to the specified recipient when an event occurs. If the recipient does not respond in the specified time period, the process does not escalate the notification. However, the process marks the associated event as failed. When you select this process as the workflow process for an event, a list of parameters appears.

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

The following fields require explanation:

User IDs

CA Process Automation user ID (CA APM or non-CA APM user) for acknowledging the notification. You can specify more than one user ID, separated with colons. Do not enter spaces between entries.

Example: This example contains a user ID (John) that is a text entry value and the mapped field {legaldoc.owner.userid}. The two items are separated with a colon. The mapped field {legaldoc.owner.userid} represents the user ID of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.userid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select User ID from the list of attributes.

```
John:{legaldoc.owner.userid}
```

Groups

CA Process Automation group name for acknowledging the notification. You can specify more than one group name, separated with colons. Do not enter spaces between entries.

Example: This example contains a CA Process Automation group name (ITAM) that is a text entry value.

```
ITAM
```

Email Addresses

Email address (or distribution list) of the recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (john.doe@company.com) that is a text entry value and the mapped field {legaldoc.owner.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.owner.emailid} represents the email address of the user in the Owner field of the Legal Document. To obtain the mapped field {legaldoc.owner.emailid}, click the Map Fields button, select the Owner link in the Add Fields dialog, and select Email Address from the list of attributes.

```
john.doe@company.com;{legaldoc.owner.emailid}
```

Email Copy Addresses

Email address (or distribution list) of the copy recipient of the email. You can specify more than one address, separated with semicolons. You can enter spaces between entries.

Example: This example contains an email address (jane.doe@company.com) that is a text entry value and the mapped field {legaldoc.requestor.emailid}. The two items are separated with a semicolon. The mapped field {legaldoc.requestor.emailid} represents the email address of the user in the Requestor field of the Legal Document. To obtain the mapped field {legaldoc.requestor.emailid}, click the Map Fields button, select the Requestor link in the Add Fields dialog, and select Email Address from the list of attributes.

```
jane.doe@company.com;{legaldoc.requestor.emailid}
```

Email Subject

Subject of the email message for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Acknowledgment required for) and the mapped field {legaldoc.documentidentifier}.

```
Acknowledgment required for {legaldoc.documentidentifier}
```

Email Message

Message of the email for the recipient. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
The Legal Document Document Identifier {legaldoc.documentidentifier} requires
your acknowledgment using the link in the Subject of this email.
```

Acknowledgment Title

Title that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier) only.

```
The Legal Document Document Identifier
```

Acknowledgment Description

Description that appears on the acknowledgment task that the user accesses in CA Process Automation to acknowledge receipt of the notification. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (The Legal Document Document Identifier) and the mapped field {legaldoc.documentidentifier}.

```
The Legal Document Document Identifier {legaldoc.documentidentifier}
```

Acknowledgment Time-out (Days:Hours:Minutes)

The amount of time that is allowed for acknowledgment after the email notification is sent. Days, hours, and minutes can be any numeric value. The format must be *days*:*hours*:*minutes* (separated with colons).

Example: This example specifies a time-out period of exactly four days.

```
4:00:00
```

Reminder Email Subject

Subject of the reminder email message. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Reminder for), the mapped field {legaldoc.documentidentifier}, and additional text entry content.

```
Reminder for {legaldoc.documentidentifier}. Acknowledgment required.
```

Reminder Email Message

Message of the reminder email. The product sends a reminder when half of the Acknowledgment Time-out period has passed. Enter text or combine text entry with mapped fields. You do not need to enter colons or semicolons to separate entries.

Example: This example contains text entry content (Reminder: The Legal Document Document Identifier), the mapped field {legaldoc.documentidentifier}, and more text entry content.

```
Reminder: The Legal Document Document Identifier {legaldoc.documentidentifier}
requires your acknowledgment using the link in the Subject of this email.
```

Make an Event Inactive

CA APM lets you make an event inactive so that the workflow provider (for example, CA Process Automation) does not send future notifications for the event. The history about important dates and events is retained.

Note: If your administrator has granted you the correct permissions, you can complete this task.

To make an event inactive

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

   The configuration of the event is enabled.
3. In the Configuration Information area of the page, select an existing global or local configuration.

   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 Event Configuration icon.

   The Events page for the selected field appears.
5. Click the Edit Record icon next to the event that you want to make inactive.
6. Select the Inactive check box.
7. Click the Complete Record Edit icon.
8. Click Save.
9. Click CONFIGURE: OFF.

   The configuration of the event is complete.

Notes

Notes are free-form explanatory text that you associate with any object, and supplement the information for an object. Notes are categorized by a *type* that you specify when you attach a note to an object. Use this information to search for objects that have a particular type of note assigned to them. For example, if another company acquires one of your primary suppliers, you can attach a company acquisition note to the company record for that supplier.

Default note types are provided for the following objects. Your administrator can define additional types.

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

Attach a Note

CA APM lets you attach a note to supplement the information for an object. For example, if another company acquires one of your primary suppliers, you can attach a company acquisition note to the company record for that supplier.

Follow these steps:

1. Click the object for which you want to attach a note. For example, click Model, Asset, Legal Document, Contact, Company, Organization, or Location.
2. Search for the list of available objects.
3. Click the object record for which you want to attach a note.
4. Click Notes on the left.
5. Click New and enter the note.
6. Click Save.

Update or Delete a Note

CA APM lets you update or delete a note that is attached to an object record.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click the object for which you want to update a note. For example, click Model, Asset, Legal Document, Contact, Company, Organization, or Location.
2. Search for the list of available objects.

3. Click the object record for which you want to update or delete a note.
4. Click Notes on the left.
5. Perform one of the following actions.
6. Update a note.
    a. Click the Edit Record icon for the note you want to update.
    b. Update the note information.
    c. Click Save.
7. Delete a note.
    a. Click the Mark for Deletion icon next to the note you want to delete.
    b. Click Save.

Chapter 3: Vendor Management

This section contains the following topics:

Vendor Management

Take control of your vendor relationships by understanding their interdependencies between your organization and among one another. CA APM lets you track and manage detailed information about the vendors with whom you do business, including contact information and their relationships to other companies. You can gather complete information about the total amount of money spent and what you will spend with a vendor, allowing you to negotiate product prices and purchases with your vendors.

Vendor management in CA APM involves working with the following objects:

- Directories (see page 79)
- Companies (see page 80)
- Contacts (see page 83)
- Organizations (see page 85)
- Locations (see page 86)
- Sites (see page 89)

Directories

Directory information is maintained in the repository so that you can locate the contact, company, location, and organization information you need for your IT assets. Having a directory offers you consistency for all of your assets to help make analysis easier. In addition, the directory serves as a contact repository when you must contact someone associated with an asset.

More information:

Locations (see page 86)
Sites (see page 89)

Companies

A *company* buys, sells, services, manages, or uses your IT assets in CA APM. You define company records for key organizations with which you have a business relationship, such as the following examples:

- Your own company, its parent company, or subsidiaries.
- IT manufacturers, vendors, escrow agents, maintenance providers, and service providers.

Before you define a company record, you must define records for the parent company, if any, and the default location, such as the headquarters. This additional information makes it easier to enter the information when defining the company record.

You can have multiple associations between locations and companies. These associations are useful to track companies with worldwide offices. For example, to track the contact details of a large vendor with worldwide offices, define location records for each office and associate them with the company record of the vendor.

You can specify one of the locations as the default location. The default location can be the headquarters of the company or the location that you contact most frequently.

Note: Although associating locations is not mandatory, it is considered good practice. Location records must exist in your repository before you can select locations for any objects.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

More information:

Associate Locations to a Company (see page 82)

Manage Companies

You can define, update, and delete company records for key organizations with which you have a business relationship. For example, you can define a company as an IT manufacturer, vendor, escrow agent, maintenance provider, or service provider.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Company.
2. Perform one of the following actions.
3. Define a company.
   a. Click New Company.
   b. Enter the new company information and click Save.

   Note: You can also define a company by copying an existing company, supplying a new name, changing the information, and saving the new company.
4. Update a company.
   a. Search for the list of available companies.
   b. Click the company that you want to update.
   c. Enter the new information for the company and click Save.

   Note: You can also view the details for an object that is related to your company, if the related object has a Browse icon. When you click the Browse icon, you leave the company page and you navigate to the related object page. To keep the company page in view and preserve the company information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.
5. Delete a company.
   a. Search for the list of available companies.
   b. Click the company that you want to delete.
   c. Click Delete and confirm that you want to delete the company.

Associate Locations to a Company

Associating multiple locations to a company is a recommended best practice to track companies with worldwide offices. For example, you can associate your company with the North America office, Latin America office, Asia Pacific office, and European office. Location records must exist before you can associate the location with a company.

Follow these steps:

1. Click Directory, Company.
2. Search for the list of available companies.
3. Click the company that you want to associate with multiple locations.
4. Click Locations on the left.
5. Click Select New to display the list of all available locations.
6. Select the company locations.
7. Click Save.

Add an Acquired Company

CA APM lets you maintain the details of the companies that you acquire and track acquisitions made by external companies. This information is useful when tracking the association between parent and subsidiary companies. For example, to understand the relationship between two companies, you can review the list of acquired companies.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Company.
2. Search for the list of available companies.
3. Click the company to which you want to add an acquired company.
4. Expand Relationships on the left and click Company Acquisition.
5. Click Select New and select a different company, other than the company previously selected.
6. Click Save.

   The acquired company is added to the list.

Add a Company Allocation

You can add a company allocation to list the software assets that your organization is internally approved to use, as specified in your software license agreement. For example, you are licensed to use 25 copies of version 4.0 of a software product in a sales office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Company.
2. Search for the list of available companies.
3. Click the company for which you want to add a company allocation.
4. Expand Relationships on the left and click Software Allocation.
5. Click Select New to search for and select an asset.
6. Click the Edit Record icon and enter the company allocation details.
7. Click Save.

   The software asset that your company is internally approved to use is added.

Contacts

A *contact* is a person or department who buys, sells, services, manages, or uses your IT assets in CA APM. Define contact records for key individuals and departments in which you have a business relationship, such as the following examples:

- Users, asset management staff, contract administrators, and IT staff.
- Representatives of other companies, such as manufacturers, vendors, escrow agents, maintenance, and service providers.

Before you define a contact record, define a company record (see page 81) to associate with the contact. Having the company record available makes it easier to add the company information when you are defining the contact record.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Contacts

You can define, update, and delete contact records for key people or departments in which you have a business relationship. For example, you can define contacts as asset management staff, contract administrators, IT staff, manufacturers, vendors, and service providers.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Contact.
2. Perform one of the following actions.
3. Define a contact.
   a. Click New Contact.
   b. Enter the new contact information.
   c. Click Save.

   Note: You can also define a contact by copying an existing contact, supplying a new name, changing the information, and saving the new contact.
4. Update a contact.
   a. Search for the list of available contacts.
   b. Click the contact that you want to update.
   c. Enter the new information for the contact.
   d. Click Save.

   Note: You can also view the details for an object that is related to your contact, if the related object has a Browse icon. When you click the Browse icon, you leave the contact page and you navigate to the related object page. To keep the contact page in view and preserve the contact information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.
5. Delete a contact.
   a. Search for the list of available contacts.
   b. Click the contact that you want to delete.
   c. Click Delete and confirm that you want to delete the contact.

Add a Contact Allocation

You can add a contact allocation to list the software assets that people in your organization are internally approved to use, as specified in your software license agreement. For example, the members of your IT department are licensed to use ten copies of version 4.0 of a software product in a development office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Contact.
2. Search for the list of available contacts.
3. Click the contact for which you want to add a contact allocation.
4. Expand Relationships on the left and click Software Allocation.
5. Click Select New to search for and select an asset.
6. Click the Edit Record icon and enter the contact allocation details.
7. Click Save.

Organizations

An *organization* is an internal department. CA APM lets you assign organizations to assets, locations, and contacts. For example, use an organization to identify the department for which an employee works.

Note: Administrators or users with administrative privileges can manage organizations. In addition, if you are using CA Service Desk Manager, you do not have to create the organization. You can use the information from the service desk.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Organizations

You can define, update, and delete an organization for an internal department, division, or external company. For example, you can define an organization for research and development, corporate finance, worldwide law, or global human resources.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Organization.
2. Perform one of the following actions.
3. Define an organization.
   a. Click New Organization.
   b. Enter the new organization information.
   c. Click Save.

   Note: You can also define an organization by copying an existing organization, supplying a new name, changing the information, and saving the new organization.
4. Update an organization.
   a. Search for the list of available organizations.
   b. Click the organization that you want to update.
   c. Enter the new information for the organization.
   d. Click Save.

   Note: You can also view the details for an object that is related to your contact, if the related object has a Browse icon. When you click the Browse icon, you leave the contact page and you navigate to the related object page. To keep the contact page in view and preserve the contact information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.
5. Delete an organization.
   a. Search for the list of available organizations.
   b. Click the organization that you want to delete.
   c. Click Delete and confirm that you want to delete the organization.

Locations

A *location* is a place where assets, companies, contacts, and legal documents are placed or situated. CA APM lets you associate locations with assets, companies, and contacts. You can define locations for the following objects:

- Assets
- Company offices and other locations where you track IT assets.

- Manufacturing companies, vendors, escrow agents, maintenance, and service providers.
- Contacts within and outside the company.

You can define multiple associations between locations and companies. The associations are useful when you want to track a large vendor with worldwide offices. For example, to track the contact details of a large vendor with worldwide offices, you can define location records for each office and associate them with the company record of the vendor. You can define location records for each office and associate them with the vendor company record.

You can specify one of the locations as the default location. The default location can be the headquarters of the company, or the location that you contact most frequently.

Note: Although associating locations is not mandatory, it is considered a best practice. Location records must exist in your repository before you can select locations for any objects.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Locations

You can define, update, or delete a location to manage the addresses of assets, contacts, and companies. For example, you can define the address for your North American office, Latin America office, and Asia Pacific office.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Location.
2. Perform one of the following actions.
3. Define a location.
   a. Click New Location.
   b. Enter the new location information.
   c. Click Save.

   Note: You can also define a location by copying an existing location, supplying a new name, changing the information, and saving the new location.

4. Update a location.
   a. Search for the list of available locations.
   b. Click the location that you want to update.
   c. Enter the new information for the location.
   d. Click Save.

   Note: You can also view the details for an object that is related to your location, if the related object has a Browse icon. When you click the Browse icon, you leave the location page and you navigate to the related object page. To keep the location page in view and preserve the location information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.
5. Delete a location.
   a. Search for the list of available locations.
   b. Click the location that you want to delete.
   c. Click Delete and confirm that you want to delete the location.

Associate Companies to Locations

Associating companies to locations is a best practice to track companies with worldwide offices. For example, you can associate your company with the North America office, Latin America office, Asia Pacific office, and European office.

Follow these steps:

1. Click Directory, Location.
2. Search for the list of available locations.
3. Click the location that you want to associate with companies.
4. Click Companies.
5. Associate the new location with the company.
6. Click Save.

More information:

Associate Locations to a Company (see page 82)

Add a Location Allocation

You can add a location allocation to list the software assets that the locations in your organization are internally approved to use, as specified in your software license agreement. For example, you are licensed to use 100 copies of version 4.0 of a software product in your North American office.

Note: You can view an audit history for this relationship.

Follow these steps:

1. Click Directory, Location.
2. Search for the list of available locations.
3. Click the location for which you want to add a location allocation.
4. Expand Relationships on the left and click Software Allocation.
5. Click Select New to search for and select an asset.
6. Click the Edit Record icon and enter the location allocation details.
7. Click Save.

   The software asset that the location is internally approved to use is added.

Sites

A *site* is a group of locations, which lets you use the new site in the location. For example, a site can be a city in which your enterprise has one or more physical locations, or a region in which you have customers that you support.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

Manage Sites

You can define, update, and delete sites. Sites specify groups of locations, such as a city in which your enterprise has one or more locations, or a region in which you have customers.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Directory, Site.
2. Perform one of the following actions.
3. Define a site.
   a. Click New Site.
   b. Enter the new site information.
   c. Click Save.

   Note: You can also define a site by copying an existing site, supplying a new name, changing the information, and saving the new site.
4. Update a site.
   a. Search to find the list of available sites.
   b. Click the site that you want to update.
   c. Enter the new information for the site.
   d. Click Save.

   Note: You can also view the details for an object that is related to your site, if the related object has a Browse icon. When you click the Browse icon, you leave the site page and you navigate to the related object page. To keep the site page in view and preserve the site information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.
5. Delete a site.
   a. Search to find the list of available sites.
   b. Click the site that you want to delete.
   c. Click Delete and confirm that you want to delete the site.

Chapter 4: Contract Management

This section contains the following topics:

Contract Management

After you negotiate contracts with your vendors, the supporting documentation is frequently archived and the terms are forgotten. Making contract information easily accessible lets you properly administer the terms of an agreement. CA APM lets you manage legal documents and standardize on terms and conditions for reporting and analysis. You can see the relationships between agreements and costs associated with vendor contracts to understand the financial impact. Finally, CA APM lets you attach electronic files or URL pages containing supporting documentation to objects, such as contract profiles, to quickly access the original document.

Contract management in CA APM involves working with the following objects:

- Legal documents (see page 91)
- Terms and conditions (see page 97)
- Attachments (see page 99)

Legal Documents

A *legal document* describes a legal relationship or agreement between two or more parties. For example, contracts, notification letters, master agreements, lease agreements, volume purchase agreements, additions to agreements, letters of intent to purchase, and so forth, are all considered legal documents.

Legal document records are based on legal templates, which your CA APM administrator defines. When you define a legal document, you start by selecting the appropriate template. Templates provide fields that apply to specific types of legal documents. Regardless of the legal template you use, you can use legal documents to track the following information:

- Record information about parties to the legal document, both primary and other parties.
- Create relationships to associate related records (for example, to associate an amendment to its original agreement).

- Store attachments with your legal document record (for example, a scanned image of a document).
- Record associated cost information.

You can retrieve information from the repository about any object by searching. You can then select, view, and manage individual object records from the search results.

More information:

Manage Legal Documents (see page 92)
Associate an Asset with a Legal Document (see page 94)
Make an Obsolete Legal Document Inactive (see page 96)
Assign and Track the Status of a Legal Document (see page 97)
Associate a Governing Legal Document with a Legal Document (see page 93)

Manage Legal Documents

You can define, update, or delete a legal document. For example, you can define a legal document for a contract or negotiation letter, or you can change the termination date for an equipment lease. You can delete a contract or lease agreement that has expired. You cannot delete a legal document that is associated with an asset.

Important! When you delete an object, you can no longer view the audit history for the object. We recommend that instead of deleting the object, you make the object inactive. Then, you can still view the audit history for the object.

Follow these steps:

1. Click Legal Document.
2. Perform one of the following actions.
3. Define a legal document.
   a. Click New Legal Document.
   b. Enter the legal document information.
   c. Click Save.

   Note: You can also define a legal document by copying an existing legal document, supplying a new name, changing the information, and saving the new legal document.

4. Update a legal document.
   a. Search to find the list of available legal documents.
   b. Click the legal document that you want to update.
   c. Enter the new information for the legal document.
   d. Click Save.

   Note: You can also view the details for an object that is related to your legal document, if the related object has a Browse icon. When you click the Browse icon, you leave the legal document page and you navigate to the related object page. To keep the legal document page in view and preserve the legal document information, right-click the Browse icon and select Open Link in New Window. Close the new window when you are finished viewing the related object details.
5. Delete a legal document.
   a. Search to find the list of available legal documents.
   b. Click the legal document that you want to delete.
   c. Click Delete and confirm that you want to delete the legal document.

More information:

Add and Remove Legal Document Terms and Conditions (see page 98)

Associate a Governing Legal Document with a Legal Document

A governing legal document is the document on which a legal document is based. CA APM lets you associate a governing legal document with the legal documents on which it is based. This association is useful when tracking the source of the legal terms and conditions of a legal document.

Note: You can view an audit history for this relationship.

To associate a governing legal document with a legal document

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document to which you want to associate a governing legal document.
4. On the left, expand Relationships and click Governing Legal Document.

5. Click Select New and select a different legal document, other than the legal document previously selected.
6. Click Save.

   The governing document is associated with the legal document.

Track Amendments to a Legal Document

CA APM lets you create and track amendments that have been made to a legal document. Save the amendments as a separate legal document and associate the amendments with the parent legal document.

Note: You can view an audit history for this relationship.

To track a legal document amendment

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to enter amendment details.
4. On the left, expand Relationships and click Legal Amendment.
5. Click Select New and select a different legal document, other than the legal document previously selected.
6. Click Save.

   The amendment details are saved.

Associate an Asset with a Legal Document

CA APM lets you associate assets and legal documents to identify the assets that a legal document covers. Initiate this association from either the legal document or asset. You can associate multiple assets to a single legal document and multiple legal documents to a single asset.

Note: You can view an audit history for this relationship.

To associate an asset with a legal document

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document that you want to associate with an asset.
4. On the left, expand Relationships and click Legal Asset.

5. Click Select New in the Legal Asset section, search for and select an asset.

   The asset name appears.

6. Click Save.

   The asset is associated with the legal document.

More information:

Terms and Conditions (see page 97)

Add and Remove Asset Legal Document Terms and Conditions

Terms and conditions are specific areas of agreement that are defined in legal documents. For example, legal documents can have terms and conditions for a multi-product discount, a new pricing model, copyright protection, and so forth. After you associate an asset with a legal document, CA APM lets you add or remove terms and conditions for the asset legal document from the Asset (see page 32) or the Legal Document page.

Note: You can view an audit history for this relationship.

To add and remove asset legal document terms and conditions

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to add or remove terms and conditions.
4. On the left, expand Relationships and click Legal Asset.
5. Click the Edit Record icon for the asset for which you want to add or remove terms and conditions.
6. Click View Assigned T's & C's.
7. Select one of the following options:
   - Click Select New for the date-specific or non-date-specific T's and C's to add to the asset legal document.
   - Click the Mark for Deletion icon for the terms and conditions that you want to remove from the asset legal document.
8. Click Save.

   The terms and conditions are added or removed.

Note: For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see the *Administration Guide*.

Associate a Legal Party with a Legal Document

CA APM lets you associate the people and entities involved in creating a legal document to the document record. For example, you can associate the lawyers and the law firm as legal parties for the legal document.

Note: You can view an audit history for this relationship.

To associate a legal party

1. Click Legal Document.
2. Search to find the list of legal documents.
3. Click the legal document for which you want to associate a legal party.
4. On the left, expand Relationships and click Legal Party.
5. Click Select New to search for and select a company.
6. Click Save.

   The company is defined as the legal party.

Make an Obsolete Legal Document Inactive

As a best practice, change the status of an obsolete legal document to inactive rather than deleting the legal document. We recommend this approach because when you delete a legal document record, the historical information for the legal document is permanently removed from the repository. In this way, you retain the legal document information for future reporting and reference.

To make an obsolete legal document inactive

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document that you want to make inactive.
4. Select the Inactive check box.
5. Click Save.

   The legal document status is changed to inactive.

Assign and Track the Status of a Legal Document

CA APM lets you assign and track the status of a legal document. For example, if the document has been signed, assign the status as executed. You can track the changes in the status of a legal document over time. The status identifies the stage of completion or implementation of the legal document.

To assign and track the status of a legal document

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to track the status.

   The legal document details appear. The status details are available in the Status section.
4. Click New in the Status section.
5. Specify the new status for the legal document.
6. Select the Current check box to indicate that the selected status is the current status of the legal document.
7. Click Save.

   The status is updated and the previous status is added to a chronological status list for the legal document. As a best practice, change the current status each time the status of a legal document changes. Only one status can be entered as the current status of a legal document. All dates are automatically updated.

Terms and Conditions

Terms and conditions are areas of agreement specified in legal documents. CA APM lets you track terms and conditions for the following reasons:

- To enforce order or comply with an existing legal document.
- To negotiate future legal documents.

Administrators and users with appropriate privileges create and maintain a master list of terms and conditions. When you work with legal documents, you use terms and conditions from this list. You can assign terms and conditions when you define legal document records or asset records.

When you define a legal document record, you start by selecting a legal template. The legal template contains the terms and conditions that typically apply to the legal document type. You can update the terms and conditions provided by the legal template to help ensure that the legal document record contains only the terms and conditions that apply.

A master terms and conditions list must exist in your repository before you can assign terms and conditions to your legal templates. You can assign a term or condition to one or more legal templates and legal document records.

Terms and conditions can be date-specific or non-date-specific. Date-specific terms and conditions include information about the start and end dates. For example, if one of your terms and conditions is Installation Date, you can have start and end date information included about the Installation Date. You determine which terms and conditions are date-specific when you create new terms and conditions in Directory, List Management.

Note: For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see the *Administration Guide*.

We recommend that you do not include the following terms and conditions in your master list:

- Effective and termination dates, as they are recorded directly on legal document records.
- Cost-related terms and conditions, as they are recorded directly on cost records.
- Software licensing terms, as they are recorded on license records.

Note: When you define an asset, you can associate the asset to the legal document records that govern the asset. The terms and conditions that apply to the legal documents also apply to the asset. If a particular asset requires terms and conditions that the legal documents do not provide, you can change the terms as you associate the asset and legal document. The legal documents covering a particular asset must contain the terms and conditions that apply only to the asset.

Add and Remove Legal Document Terms and Conditions

Terms and conditions are specific areas of agreement that are defined in legal documents. For example, legal documents can have terms and conditions for a multi-product discount, a new pricing model, or a copyright protection. CA APM lets you add the terms and conditions that are required in a legal document and remove any that are inherited from the legal template but are not required in the legal document.

Note: After you associate an asset with a legal document, you can add or remove terms and conditions for the legal document from the Asset (see page 32) or Legal Document page.

To add and remove legal document terms and conditions

1. Click Legal Document.
2. Search to find the list of available legal documents.
3. Click the legal document for which you want to add or remove terms and conditions.
4. On the left, click T's and C's.
5. Select one of the following options:
   - Click Select New for the date-specific or non-date-specific T's and C's to add to the legal document.
   - Click the Mark for Deletion icon for the terms and conditions that you want to remove from the legal document.
6. Click Save.

   The terms and conditions are added or removed for the legal document.

Note: For more information about defining date-specific and non-date-specific terms and conditions for legal documents, see the *Administration Guide*.

Attachments

Attachments are electronic files or URL pages containing supporting documentation that you associate with an object. For example, you can add an attachment of a scanned contract to the legal document record that represents the contract.

You can use the following types of attachments:

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

You can add attachments to the following objects:

- Model
- Asset
- Legal Document
- Contact
- Company
- Organization
- Location

You can add one or more attachments to an object, including spreadsheets, word-processing files, and scanned documents. In addition, you can add the same attachment with the same attachment name to multiple object records. For example, you can add an attachment of a scanned invoice to all assets listed on the invoice.

Manage an Attachment

You can add, update, and delete an attachment for an object. The following examples illustrate how you can manage an attachment:

- You can attach a scanned copy of an invoice to record all assets that are listed on the invoice.
- You can edit the URL to a scanned copy of an invoice if the location has changed.

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 server.

Follow these steps:

1. Click the tab and optional subtab for the object for which you want to manage an attachment.
2. Search to find the list of available objects.
3. Click the object for which you want to manage an attachment.
4. On the left, click Attachments.
5. **Add an Attachment.** Follow these steps:
   a. Click New.
   b. Complete the required information.
   c. In the File Path field, select a file from your local server, or enter a URL for the new attachment. For a URL, include the following prefix:

      `http://`

      If you are adding a file attachment, your selected file is copied to a CA APM server. This copy activity can take a few moments to complete. Wait for the file to finish copying before you click Save.

      Important! The file size is limited by the product environmental settings. For more information, contact your administrator or CA Support.

      Note: If you select a file that exists on the server, you are prompted to overwrite the existing file. Click Yes to overwrite the file, click No to use the existing file on the server, or click Cancel to clear the file selection.

6. **Update an Attachment.** Follow these steps:
   a. Click the Edit Record icon for the attachment.
   b. Change the information for the attachment.

      Note: For a file attachment, you can update the name and description for the attachment record. However, to update the file for a file attachment, you delete the existing attachment record and add a new attachment with a new file.
7. **Delete an Attachment.** Click the Mark for Deletion icon next to the attachment.
8. Click Save.

   The attachment is added, updated, or deleted.

Chapter 5: Software License Management

This section contains the following topics:

Software License Management

CA APM provides visibility into the software environment in your organization by tracking detailed information about software licenses. This information includes internal allocations (locations, companies, contacts, and assets), payment history, purchasing information, and the location of hard copy license agreements or attachments of the relevant license and payment documents required by an audit.

Software license management in CA APM involves working with the following objects:

- Software internal allocations (see page 103)
- Software assets (see page 107)

Important! We do not recommend that you manage software assets in CA APM. To take advantage of the enhancements that this release provides, we recommend that you use CA SAM to manage your software assets and licenses.

Software Internal Allocations

A *software internal allocation* describes how your organization is internally approved to use a software asset, as specified in your software license agreement. For example, a license can stipulate that the software can be used only on a particular computer, or that a limited number of users can use the software at one time.

You track and maintain allocations in CA APM using an allocation record. Define an allocation record for any software asset in your repository.

CA APM lets you record an allocation in the following ways:

- For a software asset, you can add, edit, or delete a relationship to a hardware asset on which the software is internally approved for use.
- For a hardware asset, you can edit or delete information about an allocation that is specific to that hardware asset.

Note: Internal allocations are not legal restrictions. Legal information, including software usage constraints, can be maintained in legal document records and in CA SAM.

More information:

Add a Location Allocation (see page 104)

Add a Location Allocation

CA APM lets you add a location allocation to list the places where your organization is internally approved to use a software asset, as specified in your software license agreement. For example, you are licensed to use 100 copies of version 4.0 of a software product in your North American office.

Note: You can view an audit history for this relationship.

To add a location allocation

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add a location allocation.
4. On the left, expand Relationships and click Location Allocation.
5. Click Select New to search for and select a location.
6. Click the Edit Record icon and enter the location allocation details.
7. Click Save.

   The location where your organization is internally approved to use the software asset is added.

Add a Company Allocation

CA APM lets you add a company allocation to list the subsidiary companies where your organization is internally approved to use a software asset, as specified in your software license agreement. For example, you are licensed to use 25 copies of version 4.0 of a software product in a sales office.

Note: You can view an audit history for this relationship.

To add a company allocation

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add a company allocation.
4. On the left, expand Relationships and click Company Allocation.
5. Click Select New to search for and select a company.
6. Click the Edit Record icon and enter the company allocation details.
7. Click Save.

   The company where your organization is internally approved to use the software asset is added.

Add a Contact Allocation

CA APM lets you add a contact allocation to list the people who are internally approved to use a software asset, as specified in your software license agreement. For example, the members of your IT department are licensed to use ten copies of version 4.0 of a software product in a development office.

Note: You can view an audit history for this relationship.

To add a contact allocation

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add a contact allocation.
4. On the left, expand Relationships and click Contact Allocation.
5. Click Select New to search for and select a contact.
6. Click the Edit Record icon and enter the contact allocation details.
7. Click Save.

   The contact who is internally approved to use the software asset is added.

Add an Asset Allocation

CA APM lets you add an asset allocation to list the hardware assets on which your organization is internally approved to use a software asset, as specified in your software license agreement. For example, the members of your IT department are licensed to use 10 copies of version 4.0 of a software product on their Dell Precision Workstation 410 computers.

Note: You can view an audit history for this relationship.

To add an asset allocation

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to add an asset allocation.
4. On the left, expand Relationships and click Asset Allocation.
5. Click Select New and select a different hardware asset, other than the asset previously selected.
6. Click the Edit Record icon and enter the asset allocation details.
7. Click Save.

   The hardware asset on which your organization is internally approved to use the software asset is added.

Delete an Allocation

CA APM lets you delete the details of an allocation record. For example, your organization purchases Adobe Acrobat Professional and internally allocates the licenses to 100 users. One user does not need the license. Therefore, you remove the software from the computer and delete the allocation. By completing these steps, you make the license available to another user in a new allocation record.

To delete an allocation

1. Click Asset.
2. Search to find the list of available assets.
3. Click the software asset for which you want to delete the allocation.
4. On the left, expand Relationships and click the appropriate allocation type.

   The allocation list appears.
5. Click the Mark for Deletion icon next to the allocation that you want to delete.
6. Click Save.

   The allocation record is deleted.

Software Assets

CA APM lets you track and manage licensing information for *software assets* that your company is entitled to use. The following fields on the Asset Details page represent the licensing information that you can manage for software assets:

- License Class
- License Count
- License Key
- License Duration
- License Duration Units

You can define and maintain this license information for software assets only.

Chapter 6: Request Management

This section contains the following topics:

Request Management

You can automate the request of IT assets through a repeatable service offering that is accessible through a service catalog. This function can increase customer satisfaction and can standardize your asset base to improve response times and service levels.

Use the CA APM integration with CA Service Catalog to automate request fulfillment.

Request Fulfillment

When CA APM and CA Service Catalog are integrated, you can perform request fulfillment using the two products. Use request fulfillment to associate requested items from a CA Service Catalog service request with CA APM assets. During the fulfillment process, you can view assets that are assigned to a request, you can assign assets to a request, and you can remove assets from a request. In addition, you can deny the fulfillment of a request for assets.

Note: For information about creating and managing requests in CA Service Catalog, see the *CA Service Catalog Integration Guide*.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

How to Fulfill Requests from Inventory

When you integrate CA Service Catalog with CA APM, you can associate assets with items requested from the catalog during request fulfillment. To fulfill requests from inventory, complete the following steps:

1. In CA APM, verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled.

   Note: For more information about creating user roles, see the *Administration Guide*.

2. In CA Service Catalog, create a request for an asset.

   The request contains information about the requester and the type of hardware or software asset being requested.

3. In CA Service Catalog, open the request and click the gold brick action icon associated with the request.

   CA APM opens and the CA APM Fulfillment page appears.

   Note: For information about creating and managing requests, see the *CA Service Catalog Integration Guide*.

4. In CA APM, complete the following steps:

   a. Search for the assets from the inventory request that you want to fulfill.

   b. Complete any of the following steps:

      - Fulfill the inventory request for a hardware asset (see page 111).
      - Fulfill the inventory request for a software asset (see page 112).
      - (Optional) Deny an inventory request (see page 113).
      - Display the list of assigned assets (see page 113) to verify that they match the request.
      - (Optional) Remove an assigned hardware asset from an inventory request (see page 114).
      - (Optional) Remove an assigned software asset from an inventory request (see page 114).

5. In CA Service Catalog, verify the status of the fulfilled inventory request.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Fulfill an Inventory Request for a Hardware Asset

You can fulfill a CA Service Catalog inventory request so that hardware assets are correctly assigned and fulfilled. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all hardware assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see the *Administration Guide*.

Follow these steps:

1. On the CA APM Fulfillment page, complete one of the following steps to search for an asset:
   a. Scroll through the list of all available hardware assets that appear in the search results.
   b. Specify the search criteria and click Go.

      A list of matching hardware assets appears in the search results.
2. In the search results, select the assets that you want to fulfill.
3. (Optional) In the Fulfillment Changes area of the page, make field-level changes to all selected assets. For example, you can change the department, cost center, general ledger (GL) code, contact, and location for all selected assets.
4. Click Fulfill.

   The request is fulfilled, the status of the request is updated in CA Service Catalog, and the asset information is updated in CA APM.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Fulfill an Inventory Request for a Software Asset

You can fulfill a CA Service Catalog inventory request so that a software asset is correctly assigned and fulfilled. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all software assets available in CA APM.

Important! If you have a CA SAM implementation, we do not recommend that you fulfill software asset requests in CA APM. To take advantage of the enhancements that this release provides, we recommend that you use CA SAM to manage your software assets and licenses.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see the *Administration Guide*.

Follow these steps:

1. On the CA APM Fulfillment page, complete one of the following steps to search for a software asset:
   a. Scroll through the list of all available assets that appear in the search results.
   b. Specify the search criteria and click Go.

      A list of matching software assets appears in the search results.
2. In the search results, click the software asset that you want to fulfill.

   The Asset Details page for the selected software asset appears.
3. Define or update software internal allocations for the software asset by clicking Asset Allocation in the Relationships menu.
4. Click New and select the hardware asset that you want to associate with the software asset.
5. Click Fulfill and Save.

   The software request is fulfilled, the internal allocations are saved, the status of the request is updated in CA Service Catalog, and the asset information is updated in CA APM.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Deny an Inventory Request

You can deny an inventory request to indicate that none of the assets requested will be fulfilled. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see the *Administration Guide*.

On the CA APM Fulfillment page, click Not Fulfilled from Inventory.

The inventory request is denied, and the status of the request is updated in CA Service Catalog.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Display Assets Assigned to a Request

CA APM lets you display all assets currently assigned to a CA Service Catalog request so that you can manage the request fulfillment. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see the *Administration Guide*.

To display assets assigned to an inventory request, click Assigned Asset in the menu on the left of the CA APM Fulfillment page.

A list of all assets assigned to the request appears in the search results.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Remove an Assigned Hardware Asset from an Inventory Request

CA APM lets you remove an assigned hardware asset from an inventory request. For example, you have a laptop that was mistakenly added to a request and you need to remove the laptop from the request. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all hardware assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see the *Administration Guide*.

Follow these steps:

1. On the left of the CA APM Fulfillment page, click Assigned Asset.

   A list of all hardware assets that are assigned to the request appears in the search results.

2. In the search results, select the hardware assets that you want to remove from the request.

3. (Optional) In the Fulfillment Changes area of the page, make field-level changes to all selected assets. For example, you can change the general ledger (GL) code, cost center, department, contact, location, and so forth.

4. Click Remove Assignment.

   The hardware asset is removed from the request, the status of the request is updated in CA Service Catalog, and the asset information is updated in CA APM.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Remove an Assigned Software Asset from an Inventory Request

CA APM lets you remove an assigned software asset from an inventory request. For example, a graphics software package was mistakenly added to a request and you remove the software from the request. When you open CA APM from a CA Service Catalog request, the CA APM Fulfillment page appears with a list of all software assets available in CA APM.

Note: Verify that the user fulfilling the request belongs to a role in which asset fulfillment access is enabled. For more information about creating user roles, see the *Administration Guide*.

Follow these steps:

1. On the left of the CA APM Fulfillment page, click Assigned Asset.

   A list of all software assets that are assigned to the request appears in the search results.

2. In the search results, click the software asset that you want to remove from the request.

   The Asset Details page for the selected software asset appears.

3. Remove or update software internal allocations for the software asset by clicking Asset Allocation in the Relationships menu.

4. Click the Delete icon next to your selected asset.

5. Click Remove Fulfillment and Save.

   The asset is removed from the request, the internal allocations are saved, the status of the request is updated in CA Service Catalog, and the asset information is updated in CA APM.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Chapter 7: Audit History

This section contains the following topics:

Audit History

An *audit history* is a chronological list of changes made to an object record over time. Auditing records all changes made to each field in an object record. CA APM lets you use an audit history to view a list of all changes made to a record.

You can use an audit history to see the changes made to the value of a particular field and see who changed the value. If a field contains an incorrect entry or value, use the audit history to verify the last correct value and update the object record.

The following objects enable auditing by default and without any additional configuration:

- Models (including Model Pricing)
- Assets
- Companies
- Contacts
- Organizations
- Locations
- Sites
- Legal Documents (including Terms and Conditions)
- Legal Assets (including Terms and Conditions)
- Costs
- Payments
- Relationships
- Asset Configurations (Models and Assets)
- Software Internal Allocations (Locations, Companies, Contacts, and Assets)

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

View an Audit History of Object Changes

CA APM lets you view an audit history for an object record to see a list of all of the changes that have been made to the record. The audit history maintains and shows you the historical information so that you are aware of all of the changes that have been made to the object.

Example: Review the Audit History to Change the Cost Center

In this example, a line manager discovers that the incorrect department is being charged for a laptop. The line manager investigates the situation and determines that the laptop is assigned to the incorrect cost center. To understand how this error occurred, the line manager configures and filters the audit history search criteria and results for the laptop to include the cost center. The line manager reviews the audit history for a specific time period to determine when the cost center value changed and who changed the value. The line manager contacts the asset manager to have the cost center changed to the correct value.

To view an audit history of object changes

1. Click the tab and optional subtab for the object for which you want to view an audit history.
2. Search to find the list of available objects.
3. Click the object in the search results for which you want to view an audit history.
4. Click View Audit History.

   Note: To view the audit history for a relationship, select the relationship (for example, Image Partitions), click the Edit Record icon, and click View Audit History.

   All changes made to the object record appear.

5. (Optional) Complete any of the following steps in the Search Criteria area of the page to filter the audit history search results:

   a. Select a specific field in the Target Field drop-down list and click Go.

      The Search Results are limited to the field that you select. In addition, the standard auditing fields appear to identify the user who changed the field, to identify the type of change (insert, update, and so forth), and to identify the date on which the change is made.

   b. Select the Highlight Changes check box and click Go.

      The Search Results highlight changes in adjacent rows. You can use this check box, in combination with a specific field in the Target Field drop-down list, to identify field-level changes that you may need to correct.

6. Export the audit history to a CSV file or click the hyperlink to return to the object details.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

View an Audit History of Events

CA APM lets you view an audit history of all events created for an object. For example, you define a date event on the Terminate Date field for a legal document and a notification for the event is sent to the appropriate person on 3/1/2010. The audit history maintains the event history for an object and displays this information so that you are aware of all events created for the object.

To view an audit history of events

1. Click the tab and optional subtab for the object for which you want to view an audit history.
2. Search to find the list of available objects.
3. Click the object in the search results for which you want to view an audit history.
4. Click View Audit History.

   All changes made to the object record appear.

5. In the audit history results, click the icon in the Event History column.

   All events and their associated status (see page 120) created for the audit record appear.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)

Event Status

When you view an audit history of events (see page 119), you can see the associated status for each event.

Event Status	Description
Unprocessed	CA APM has created the event, but the event has not been processed to map the workflow process attributes for notifications in CA Process Automation.
Started	The mapping for the workflow process attributes in CA Process Automation is complete, and the associated notification process for the event has started.
In Progress	The CA Process Automation notification process for the event is processing.
Completed	The CA Process Automation notification process for the event is completed.
Failed	The CA Process Automation notification process for the event has failed.
Aborted	The CA Process Automation notification process for the event has stopped.

Chapter 8: Reporting

This section contains the following topics:

Reconciliation Reports

Use the reconciliation reports to view the following information and help you manage your IT assets based on your business practices:

Note: Your security permissions determine the tenant data you see when generating reports. If you have access to multiple tenants, you see the data for all tenants to which you have access. If you only have access to a single tenant, you only see the data for that tenant.

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

Generate a Report

CA APM reports provide you with a detailed view of your owned and discovery assets to help with reconciliation.

Important! If you plan to add to your repository using the Data Importer the discovered assets that are not matched to any of your owned assets, select only a single tenant when generating the appropriate report.

To generate a report

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 you want to generate.
6. Enter the search criteria for the report.
7. Click Run Query.

Remove the Tenant Drop-Down List

Any user belonging to more than one tenant can select a tenant in a drop-down list when generating a report. You can remove the tenant drop-down list so that you are not asked to select a tenant when generating a report.

To remove the tenant drop-down list

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.

   All CA APM reports appear.
5. Right-click the report for which you want to remove the tenant drop-down list and select Modify.

   The Prompts dialog opens.
6. Click Cancel.

7. Click Edit Query.
8. At the bottom of the page in the Query Filters area, right-click the Tenant - Multi-Mandatory filter and select Remove.
9. Repeat the previous step for all tabs. Tabs appear below the Query Filters area of the page.

   Note: All CA APM reports, except the Reconciliation Metrics report, have only one instance of the Tenant - Multi-Mandatory filter. The Reconciliation Metrics report has six instances of the Tenant - Multi-Mandatory filter on different tabs that you must remove. Remove all instances of the filter on the report for the selected values and Report Strings tabs.
10. Click Edit Report.
11. Click the Save icon.
12. Save the report in the same location from where the report is opened.
13. When prompted, click Yes to override the existing report.
14. Click the Close document icon.

    When you generate the report, you are not asked to select a tenant.

Chapter 9: Searching

This section contains the following topics:

Object Searching

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. At any time, you can search to find objects in the repository to manage. You can also search the audit history to see all changes made to an object record over time.

For example, you can search for objects for the following reasons:

- Search for a model so that you can define an asset from the model.
- Search for an asset so that you can define a support contact for the asset.
- Search for an asset from an inventory request that you want to fulfill.
- Search for a legal contract so that you can define terms and conditions for the contract.
- Search the audit history so that you can see when the cost center for a laptop changed, and who changed the cost center.

Based on the search criteria that you specify, a list of matching objects appear in the search results.

Most of the time, the objects that you want to view or update appear with the default search provided for each object. This type of search is intended for when you want to locate a single record for update from a simple list of objects. For example, you can enter the serial number when searching for a laptop to find the laptop matching the serial number.

When you search, you can use search operators (see page 130) and search connectors (see page 131) to make your searches more precise and get more useful results.

More information:

Delete a Search (see page 134)
Update a Search (see page 132)
Search for Objects Using a Saved Search (see page 133)
Save a Search (see page 132)
Sort the Search Results (see page 131)
How to Configure Searches (see page 144)
Copy a Search (see page 133)
Search Results Export (see page 134)

Search Tips

Use the following information and techniques to help make your searches more effective:

- **Keep it simple**. For example, if you are looking for a specific asset or model, and you have the name available, enter the name. If you have additional information to identify the object, such as the serial number for an asset, enter that number. This additional information increases the chance that your search returns the object you want.
- **Expand your search with a wildcard**. Use the asterisk (*) or percent sign (%) wildcard character as a substitute for any number of characters in your search string to return search results. Use as many wildcard characters in your search string as you want. For example, enter *S** or *S%* when searching for contacts by last name to find contacts having the last name Sanders, Shelley, Smith, Spencer, Solomon, and so forth. Enter *Dell *" Monitor* when searching for assets by name to find any size Dell monitor; Dell 19" Monitor, Dell 21" Monitor, Dell 30" Monitor, and so forth.
- **Searches are not case-sensitive**. You can ignore capitalization in your searches. For example, a company search for *Document Management Company* returns the same results for *document management company.*
- **Search titles are unique in a tenant**. When you save a search and specify a title, the title must be unique within a tenant. You cannot save a search with the same title in a single tenant.
- **If you receive too many, or too few, search results** and cannot find an object, try the following suggestions:
  - Use different search criteria. For example, instead of searching for a contact by last name, search for their first name, department, user ID, or location.
  - Use operators (see page 130) and connectors (see page 131) to increase or decrease the objects returned in the results.
  - Verify that you have spelled the name of the object correctly, and have entered any additional search criteria correctly.

- **Expand your search with check box criteria**. Include check box fields such as Inactive in your searches. For example, search for all inactive assets and generate a report for management analysis. You can also search for all inactive assets to make them active again.
- **Expand your search within multiple asset families and legal template types**. Search within one or more asset families and legal template types. For example, search for a specific model under both hardware and software, or search for a legal document under a service contract and software addition.
- **Invalid Searches**. You can use the Invalid drop-down list when you manage searches to display or hide invalid searches. A search becomes invalid when your CA APM administrator configures the user interface and restricts access to any field that a search uses, or deletes an extended field that a search uses. If you have a search that you cannot use because of security restrictions, contact your CA APM administrator for assistance.
- Sort the search results (see page 131) to help make it easier to find information.
- Save a search (see page 132) you frequently use so that you do not have to enter the search criteria each time you use the search.
- Copy a search (see page 133) and use the search as a template for creating another search that is similar.
- Export search results (see page 134) for use in spreadsheet applications or reports.
- Configure your searches (see page 144).

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 *user-defined searches*.

Consider the following security information for user-defined searches:

- 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 you see for the default searches do not display information and fields that your CA APM administrator hides and secures.
- When you configure the user interface and restrict access to any field that a search uses, or delete an extended field that a search uses, the search is invalid. As a result, the search is not available to any user that is associated with the role and configuration.

- Invalid and active searches appear together when you manage searches. When you try to use an invalid search, you receive a message. You should contact your CA APM administrator to troubleshoot the invalid search and make the search valid again.
- When a search becomes invalid, you may have no default search. When attempting to search, you receive a message. You should contact your CA APM administrator to have a default search assigned, or you can save a new search and set the search as your default search.

Example: Limit Asset Searches by Cost Center and General Ledger Code

In this example, an asset in your organization is assigned to a particular cost center and general ledger code. This information is used to identify the department responsible for the expense, and to allocate costs on order releases, shipments, and payment invoices. This information is sensitive and should not be available to all users who search for assets in your repository.

You can copy the default asset search and configure the search by adding the cost center and general ledger code to both the search criteria and search results. When you save the new configured search, you assign the search to only those individuals in your finance and procurement department (that is, users assigned to the finance user role). Users in the finance user role can now search and find assets based on the cost center and general ledger code. Users not assigned to this role cannot search for an asset using that information.

More information:

Object Searching (see page 125)
How to Configure Searches (see page 144)
Search Results Export (see page 134)
Troubleshooting Search Security (see page 154)

Search for Objects

At any time, you can search to find objects in the repository to manage. For example, you can search for a model and define an asset from the model. Based on the search criteria that you specify, a list of matching models appear in the search results.

To search for objects

1. Click the tab and optional subtab for the object that you want to find.
2. In the Search Criteria area, specify the search criteria.

3. (Optional) In the Search Criteria area, click Advanced.
4. Click the Edit icon to specify the search criteria:

   Left Parenthesis

   Determines if left parentheses are used to group search criteria and control the logic of the search. For example, you can select this check box to search for assets in which the asset name is OE001 or both the asset family is Computer and the asset name is Dell.

   Operator

   Determines the standard search operators (see page 130) to use to find objects. For example, you can search for assets in which the asset name is greater than OE001 and the asset family is Computer.

   Value

   Determines the specific field value that you want to find. For example, you can search for an asset in which the asset name is OE001.

   Note: When you enter a search value in combination with the Like or Not Like operators, you can use all supported wildcard characters to expand your search.

   Right Parenthesis

   Determines if right parentheses are used to group search criteria and control the logic of the search. For example, you can search for assets in which the asset name is OE001 or both the asset family is Computer and the asset name is Dell.

   Connector

   Determines the standard connectors (see page 131) to use to find objects. For example, you can search for assets in which the asset name is OE001 or both the asset family is Computer and the asset name is Dell.
5. Click the Complete icon to accept your search criteria changes.
6. Click Go.

   A list of matching objects appears in the search results.

More information:

Delete a Search (see page 134)
Update a Search (see page 132)
Export Search Results to a CSV File (On Demand) (see page 137)
Search for Objects Using a Saved Search (see page 133)
Save a Search (see page 132)
Sort the Search Results (see page 131)
How to Configure Searches (see page 144)
Copy a Search (see page 133)

Search Operators

When you search for objects, CA APM lets you use the following standard search operators to find objects in the repository:

Operator	Description
Equal	Search for objects having the exact value specified.
Not Equal	Search for objects not matching the value specified.
Greater Than	Search for objects greater than the value specified.
Greater Than or Equal	Search for objects greater than or equal to the value specified.
Less Than	Search for objects less than the value specified.
Less Than or Equal	Search for objects less than or equal to the value specified.
Like	(Similar) Search for objects that match the value specified. When you use the Like search operator, the % wildcard is added after the characters you enter and searches for all objects that start with the characters. You can also add the % wildcard before the characters to search for all objects that end with the specified characters. **Note:** When you enter a search value in combination with the Like or Not Like operators, you can use all supported wildcard characters (see page 126) to expand your search.

Operator	Description
Not Like	(Not Similar) Search for objects that do not match the value specified. When you use the Not Like search operator, the % wildcard is inserted after the characters you enter and searches for all objects that do not start with the characters. You can also insert the % wildcard before the characters to search for all objects that do not end with the specified characters. **Note:** When you enter a search value in combination with the Like or Not Like operators, you can use all supported wildcard characters (see page 126) to expand your search.

Search Connectors

When you search for objects, CA APM lets you use the following standard AND/OR connectors to connect search strings and find objects in the repository.

AND

The search must satisfy the criteria for both the current search field and the following search field.

OR

The search must satisfy the criteria for either the current search field or the following search field.

Sort the Search Results

CA APM lets you sort the search results to help make it easier for you to find the information in your search results. For example, you can sort the results in ascending order by asset family to find assets in the hardware asset family first, followed by assets in the software family.

To sort the search results

1. Search for objects.

   The search results appear.

2. In the Search Results area, click the appropriate icon next to a column heading.

   The sort results appear in either ascending or descending order.

   Note: You can extend the default sort of a single column by adding sort fields (see page 152).

Save a Search

CA APM lets you save a search that you frequently use so that you do not have to enter the search criteria each time you use the search. For example, you can save a search to find assets by asset name, asset family, model, cost center, and creation date.

To save a search

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

   The Add Fields dialog appears.
3. Specify the fields to appear in the search criteria and results.

   Note: When you search within multiple asset families and legal template types, only the assets, models, and legal documents for the selected families and template types appear in the search results.
4. At the top of the page, click CONFIGURE SEARCH: OFF.

   The configuration of the search is complete.
5. In the Search Details area of the page, specify the information to uniquely identify the search.

   Note: When you save a search and specify a title, the title must be unique within a tenant. You cannot save a search with the same title in a single tenant.
6. In the Search Security area of the page, select the user roles for which the search is available. Roles are helpful so you can make the search available to all users having the roles you select. Administrators can also select specific configurations for the search.

   Note: If you do not select either a role or configuration, the search is available to the current user.
7. Click Save.

   The search is saved and is available for future searches.

Update a Search

CA APM lets you change the search criteria in a saved search. For example, you can add the contact ID to a saved asset search.

To update 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 update.
4. Update the search criteria.
5. (Optional) In the Search Security area of the page, select the user roles for which the search is available. Roles are helpful so you can make the search available to all users having the roles you select. Administrators can also select specific configurations for the search.

   Note: If you do not select either a role or configuration, the search is available to the current user.
6. Click Save.

   The updates to the search are saved and available for future searches.

Search for Objects Using a Saved Search

CA APM lets you search for objects using a saved search. For example, you can use a saved weekly asset search to find all assets that have been added during the past week.

To search for objects using 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 use.
4. Click Go.

   A list of matching objects appears in the search results.

Copy a Search

CA APM lets you copy a saved search and use the search as a template for creating another search that is similar. For example, you can copy the default asset search and add the asset creation date and user ID of the person who created the asset.

To copy a 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 copy.
4. Click Copy.

   A new search is created based on the copied search.

5. Change the information for the new, copied search.
6. (Optional) In the Search Security area of the page, select the user roles for which the search is available. Roles are helpful so you can make the search available to all users having the roles you select. Administrators can also select specific configurations for the search.

   Note: If you do not select either a role or configuration, the search is available to the current user.
7. Click Save.

   The search is saved and is available for future searches.

Delete a Search

CA APM lets you delete a saved search that you do not need. You cannot delete the default searches provided by the product.

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.

Search Results Export

CA APM lets you export the results of an object, asset fulfillment, and audit history search so that you can report on and analyze the search results. For example, the asset manager, purchasing manager, and facilities manager require a weekly report that lists all of the assets that have been added during the past week. Based on this requirement, the administrator configures the search to return the list of assets and schedules the search and export to process at 10 p.m. every Friday. After the search and export processes, the managers receive an email notification that includes a link to the weekly report.

You can export the results of a search to the following formats:

- CSV file (see page 135)
- Database view (see page 136)

You can schedule a search and export (see page 138) for a particular time and automatically notify contacts by email so that the contact can access the latest information.

More information:

How Exported Search Results are Retained and Purged (see page 141)
How Exporting Search Results Works (see page 136)

CSV File Export

When you export search results to a CSV file, the export includes the current data found by the search. CA APM lets you use the following methods to export to a CSV file:

- On demand export (see page 137) from a real-time search. This type of search includes the current data.
- Scheduled export (see page 138) from a saved search. This type of search includes the current data found each time you use the search according to the schedule.

Example: Export a Search for New Assets to a CSV File

In this example, a company adds new assets to its repository every week. The asset manager, purchasing manager, and facilities manager require a weekly report that lists all of the assets that have been added during the past week. Based on this requirement, the administrator configures the search to return the list of assets and schedules the search and export to process at 10 p.m. every Friday. After the search and export processes, the managers receive an email notification that includes a link to the weekly report.

More information:

How Exported Search Results are Retained and Purged (see page 141)
How Exporting Search Results Works (see page 136)

Database View Export

When you export search results to a database view, the export contains the SQL statement that defines the columns and data in the search. The view does not collect data until you (or an external application) access and use the view in the database.

You can schedule the export from a saved search (see page 138) to export to a database view.

Example: Export a Search for Expiring Assets to a Database View

In this example, a company develops an external dashboard application that monitors asset allocation. The asset manager views the dashboard daily to verify that expiring assets are allocated properly - reallocated, retired, or returned to vendor. The company wants to configure the dashboard application to display CA APM asset data.

Based on these requirements, the administrator configures the search to display the list of expiring assets and their status and exports the search results to a database view. The administrator schedules the search and export to process weekly. The external dashboard application accesses the database view to gather the asset data, and the asset manager views the data in the external dashboard.

More information

How Exported Search Results are Retained and Purged (see page 141)
How Exporting Search Results Works (see page 136)

How Exporting Search Results Works

When you export search results to a *CSV file*, the process uses the following general steps:

1. The user defines a new search and exports the results; or the user accesses an existing saved search and schedules the export.
2. The search processes and the results include the current data.

   Note: The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

3. The search results data is saved to a CSV file. The column heading labels in the CSV file (if requested with the export) match the column heading labels from the search results. If the user configured the default column heading labels in the search results, the configured labels are included in the CSV file.
4. An email notification is sent to the users assigned to the search. The email includes a link to the CSV file.

When you export search results to a *database view*, the process uses the following general steps:

1. The user accesses an existing saved search and schedules the export.
2. The search processes and the database view is exported. The column heading labels in the database view match the column heading labels from the search results. If the user configured the default column heading labels in the search results, the configured labels are included in the database view.

   Note: The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.
3. An email notification is sent to the users assigned to the search. The email specifies the name of the database view.

Export Search Results to a CSV File (On Demand)

CA APM lets you export the results of a search to a CSV file by searching for objects and exporting the results on demand or by scheduling a saved search (see page 138) and exporting the results.

To export search results to a CSV file (on demand)

1. Click the tab and optional subtab for the object that you want to find.
2. Search for objects by entering search criteria or by selecting a saved search.

   A list of matching objects appears in the search results.
3. Click Export to CSV.

   The search results are exported. The column heading labels in the CSV file match the column heading labels from the search results. An email notification with a link to the CSV file is sent to all contacts associated with the export request.

Export Search Results to a Database View

CA APM lets you export the results of a search to a database view by scheduling a saved search and exporting the results.

To export search results to a database view

1. Click the tab and optional subtab for the object for which you want to schedule a search and export.
2. On the left, click Manage Searches.

   A list of saved searches appears. If there are no saved searches, define and save a search that you want to schedule and export.
3. Click the search that you want to schedule and export.
4. On the left, click New Export.
5. Enter the basic information, schedule information, and security information as described in the steps to schedule the search and export (see page 138).

   The search is processed and the results are exported according to the schedule. The column heading labels in the database view match the column heading labels in the search results. An email notification specifying the database view name is sent to all contacts associated with the export request.

   Note: The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

Schedule Searches and Exports

CA APM lets you schedule searches to process periodically and export the search results to a CSV file or a database view. For example, you can schedule a search to process at the end of the week and export all updated assets during that week to a CSV file. You can schedule the following types of searches:

- **Predefined**. Specify a recurring time for the search. For example, you can process the search at 3:00 p.m. on the 21st of every month.
- **Calculated**. Specify the start time and frequency for the search. For example, you can process the search at 10:00 p.m. on the 21st of September and use the search every five days thereafter.

To schedule a search and export the results

1. Click the tab and optional subtab for the object for which you want to schedule a search.
2. On the left, click Manage Searches.

   A list of saved searches appears. If there are no saved searches, define and save a search that you want to schedule and export.
3. Click the search that you want to schedule.
4. On the left, click New Export.
5. Enter the basic export information.

   The following fields require explanation:

   Export Name

   Specify the export name.

   Export Format

   Select the format for the exported search results.

   View Name

   Specify the database view name.

   Note: The View Name is required if you select Database View for the Export Format. The name must be a valid database view name. See your database product documentation for information about database view name requirements.

   Description

   Specify a description for the exported search results.

   Retention Days

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

   Folder Name

   Specify the folder for the exported CSV file search results.

Never Expires

Select this check box to specify that the number of days of the selected period (Period Type) that the CSV file or database view is stored before being deleted never expires (the CSV file or database view is never purged). When you select this check box, any previous value that you added to the Retention Days field is removed, and the Retention Days field is disabled.

6. Schedule the search.

The following fields require explanation:

Run Time

Select the time of the day, in 24-hour format, to process the search. When you schedule searches, use the local time zone on the CA APM application server.

Interval Type

Select the type of interval for the search. For example, you can select Day, Month, Quarter, Week, or Year.

Interval Day

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

First Run Date

Select the date when the first search starts to process.

Interval

Specify how often the search processes, based on the specified Interval Type. For example, if the Interval Type is Weekly and the Interval is 2, the search processes every two weeks.

Last Day of Interval

Select this check box to specify that the search processes on the last day of the selected Interval Type. When 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.

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

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

   Note: The results for a scheduled search and export only include the results found by the current search and export. If you change the search or any part of the export criteria, you will not see the new search results until the next time the search and export process runs. For example, if you change the Export Format from CSV File with Column Headers to Database View or you change the Frequency of the Export Schedule, you do not see those changes in the current search and export.

How Exported Search Results are Retained and Purged

All exported CSV file and database view search results are retained and purged based on configuration settings you specify when you schedule searches and exports (see page 138). The exported search results that are no longer needed are purged to release disk space.

The following information describes how exported search results are retained and purged:

- You specify the retention days when you schedule searches and exports. After the retention days elapse, the exported search results (CSV files and database views) are considered expired and are purged.
- The Export Service processes the purge once a day (by default, 5:00 a.m. Universal Time) and purges exported search results based on the specified retention days. Your administrator can configure the purge start time.

  Note: For information about the Export Service configuration settings, see the *Administration Guide*.
- The retention period depends on the processing time of the export and the time at which the Export Service purges the search results.

Example: Purge Search Results

In this example, you schedule an asset search named Weekly Asset Search to process every Friday and export all updated assets during the week. You set the retention days to 1 and the export completes at 5:00 p.m. Eastern time. The Export Service is scheduled to purge search results at midnight, Eastern time. Because the search results are less than one day old, the Export Service does not purge them until the next scheduled time (in this example, shortly after midnight the following day).

Search Results Mass Change

You can perform the following mass changes on a search results list:

- Change the value of a specific field for all objects or for selected objects in the list.
- Add a value to a specific field for all objects or for selected objects in the list that have blank values in that field.

Note: The following restrictions can affect the mass change functions that you can perform:

- Configuration restrictions for your user role. For example, if your configuration does not allow you to modify a particular field, you cannot perform mass changes on that field.
- Multi-tenancy. If you have a multi-tenanted environment, the tenant name can be a part of the search results list. However, you cannot perform a mass change on the tenant name.

Example: Perform a mass change on the cost center

A data center administrator wants to assign all assets in the London data center to cost center 3218. The administrator configures the search to return a list of all assets in the London data center. The administrator then performs a mass change to change the cost center assignment for the assets to 3218.

How the Search Results Mass Change Works

When you perform a mass change on a search results list, the process uses the following general steps:

1. The user defines a new search, selects an existing search, or uses the default search.
2. The search processes and the results appear.
3. The user defines the mass change settings for all fields or selected fields and executes the mass change.

   Note: The user must be assigned to a configuration that permits mass changes.
4. The mass change job is created and displayed in the Mass Change Jobs list.
5. The user verifies the status of the mass change job and performs the original search again when the job is completed.
6. The search results list data is updated to show the new field values.

Perform a Mass Change on a Search Results List

You can change specific field values for all or selected objects in a search results list.

Follow these steps:

1. Click the tab and optional subtab for the object that you want to find.
2. Search for objects by entering search criteria or by selecting a saved search.

   A list of matching objects appears in the search results.
3. Leave all objects selected, or clear the Select All check box and select specific object check boxes.
4. Click Mass Change Settings.
5. Click New.
6. Enter the information to define the mass change. The following fields require explanation:

   Mass Change Field

   Specifies the field in the search results that you want to change.

   Note: The fields that are included in the search results list are available for selection.

   Value

   Specifies the new value for the selected field.

   Note: Leave the Value field blank to specify a null value for a field.

   Update Only Blank Values

   Specifies that only blank values in the selected field are updated with the new value for the selected objects.
7. Click the Complete Record Edit icon.
8. (Optional) Click New to define more mass change settings.
9. Click the Mass Change button above the search results list when you have defined all mass change settings.

   A mass change job is created.
10. Click Mass Change Jobs on the left to see the Mass Change Jobs list.

    Note: You can click Go to update the jobs list.

11. Click Status Message for your mass change job to verify when the processing is completed.
12. Click View Log for your selected job in the Mass Change Jobs list after the job is completed.

    The log file provides more information about the mass change job activity.
13. Perform your original search again.

    The search results display the new field values.

How to Configure Searches

CA APM lets you configure object, asset fulfillment, and audit history searches to simplify how you search for information in the repository. To configure searches, complete the following steps:

- Set a search result limit (see page 145).
- Make it easier to search by specifying a default search (see page 145).
- Make it easier to specify search criteria by completing the following tasks:
  - Adding fields (see page 146)
  - Removing fields (see page 146)
  - Moving fields (see page 147)
  - Changing the field name (see page 148)
  - Replacing fields (see page 149)
- Make it easier to find information in the search results by completing the following tasks:
  - Adding columns (see page 149)
  - Moving columns (see page 150)
  - Changing the column label (see page 151)
  - Removing columns (see page 152)
  - Adding sort fields (see page 152)
  - Preventing duplicate records from appearing (see page 153)
  - Preventing the ability to open records (see page 153)

More information:

Audit History (see page 117)

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.

Specify a Default Search

CA APM lets you specify a search that you frequently use as the default each time you click a tab or subtab. For example, to find the contact search you click Directory, Contact. You copy the contact search, rename it, and then set it as your default. The next time you access the Contact Search page, the default search appears instead of the previous search.

Note: You cannot specify a search as the default when the search does not have a selectable column in the results.

To specify a default 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 a search in the list.
4. Click Set As Default.

5. Click Save.

   The search is saved as the default.

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*.

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.

Troubleshooting Search Security

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

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.

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.