CA Performance Center

Administrator Guide

2.4.1

CA Technologies Product References

This document references the following CA Technologies products and components:

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA NetQoS® Performance Center
- CA Single Sign-On
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor
- CA eHealth
- CA Spectrum

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: Introducing CA Performance Center

This section contains the following topics:

About CA Performance Center

CA Performance Center is a web-based reporting interface that helps you effectively manage your physical and virtual networks, applications, and devices. CA Performance Center dashboards and reports present performance data from network and systems-monitoring products. You can compare large amounts of statistical data from multiple sources in one web page.

CA Performance Center takes a "performance-first" approach to application service delivery. This approach places end users in the primary role. To understand how well an IT organization supports application delivery to users, you must capture and analyze data from applications, devices, and the network.

CA Performance Center offers role-specific views of application response times, traffic composition, infrastructure health, and flow-based diagnostics.

Data Collection

CA Performance Center relies on data sources for performance data, device identification, and device, server, and system status. Supported data sources collect various types of data: end-to-end application response times, packets, network traffic flows, and infrastructure statistics from device MIBs. Minimizing management overhead, CA Performance Center uses embedded network instrumentation and passive collection appliances running in the data center. Remote probes and agents are not used. Instead, data sources such as SNMP and NetFlow provide data from widely varying architectures.

CA Performance Center displays data from multiple sources that gather, store, aggregate, and analyze performance data from physical and virtual systems. CA Performance Center also lets you directly access the products that provide the data without requiring reauthentication.

To transform the wealth of data and analytics into actionable information, CA Performance Center provides a single reporting interface. Dashboards and alerts can be tailored to the needs of network engineers, Operations staff, server and application teams, and IT executives. You can build customized views in many formats.

Launch CA Performance Center

Once you have run the CA Performance Center Setup program and the installation has completed, you can launch the console program from a web browser.

Follow these steps:

1. Open a web browser.
2. In the address field, enter the following address:

   `http://<server IP address>:8181/pc/desktop/page`

   <server IP address>

   Is the IP address of the computer where you installed the software.

   8181

   Is the port number.

   The browser displays the Login page.
3. Type your CA Performance Center username and password in the fields provided.
4. (Optional) Select 'Remember me on this computer' to remain logged in beyond the timeout period that the administrator has set.
5. Click Log In.

   The CA Performance Center console opens to your home dashboard.

Chapter 2: Setting Up CA Performance Center

This section contains the following topics:

How to Set Up CA Performance Center

The only requirement for using CA Performance Center is the adding of supported data sources, also known as data source registration. However, you can customize your environment to make reporting more useful.

We recommend the following workflow to set up CA Performance Center:

1. Plan a group structure and naming conventions. For more information, see Creating and Managing Groups (see page 61).

   (Optional) Plan tenant structure and naming conventions. Tenants, which are used in MSP environments, let a single instance of CA Performance Center monitor multiple, discrete enterprises. For more information, see Creating and Managing Tenants (see page 125).

2. Plan the user accounts and roles that you need for CA Performance Center operators. For more information, see Creating and Managing User Accounts (see page 115) and Creating and Managing Roles (see page 89).

3. List the dashboards and menus suitable for each role. For more information, see Organizing Dashboards in Menus.

4. Register data sources. For more information, see Register a Data Source (see page 25).

5. Configure an email server so that CA Performance Center users can send report pages as email messages. For more information, see Set the Email Server (see page 12).

6. Create SNMP profiles to pass security information to data sources that poll device MIBs. For more information, see Add an SNMP Profile (see page 31).

7. (Optional) Create business-hour definitions to differentiate reported data according to its impact on business activities. For more information, see About Business Hours (see page 55).
8. Create groups of managed items. For more information, see Create a New Group (see page 73).
9. Create roles, and assign menus to roles. For more information, see Add a Role (see page 104).
10. Create user accounts, and assign roles and permission groups to these accounts. For more information, see Add a User Account (see page 121).
11. Create menus containing dashboards for reporting. For more information, see Add a Menu.
12. (Optional) Log in to each user account to test the level of access being granted to each user. For more information, see Proxy a User Account.
13. (Optional) Create tenants to represent all customer enterprises. For more information, see Add a Tenant (see page 130).
14. (Optional) Add a custom logo to a tenant theme so that exported reports include your logo in the header. For more information, see Customize a Theme (see page 13).
15. (Optional) Change Display Settings to show aliases instead of item names in dashboards. For more information, see Display Settings (see page 15).
16. (Optional) Set up event notifications. For more information, see Notifications (see page 50).

Set the Email Server

Configure an email server so that users can send reports by email. Reports can be emailed on a schedule or as needed. Select a server to which the CA Performance Center server has network access.

Follow these steps:

1. Log in as a user with administrative role rights (see page 95).
2. Select Admin, System Settings, and click Email Server.

   The Email Server Settings page opens.
3. Select the Enable Email check box.

   The page refreshes to highlight the required field.

4. Complete the following fields as necessary:

   SMTP Server Address

   Is the IP address or hostname of the server to use to send reports by email.

   SMTP Server Port

   Is the port on the email server that is used to send messages.

   Default: Port 25.

   Email Reply Address

   Is the email address from which CA Performance Center sends reports.

   Note: An administrator should monitor this address for responses to email messages sent by the product.

5. (Optional) Enable SSL encryption. This parameter is required if you want to use a secure connection to send email from CA Performance Center.
6. (Optional) Take the following steps to enable SMTP authentication:
   a. Select Enable Authentication.
   b. Type the username for SMTP authentication in the Username field.
   c. Type the authentication password in the Password field.
   d. Type the authentication password again in the Confirm Password field.

   Note: SMTP authentication is disabled by default.
7. Click Save.

   The email server is set.

Customize a Theme

Themes affect the appearance of exported reports. By default, all themes use the CA Technologies corporate logo. You can customize a theme to use a logo that you select.

Themes are typically applied per tenant. You customize a theme and assign that theme to a tenant. The custom logo appears in report headers (in PDF format) that tenant users print or send by email. If you do not deploy multi-tenancy, the theme applies to the default tenant.

Only global administrators can apply custom logos to themes. If you are not deploying multi-tenancy, log in as a user with the predefined Administrator role.

Follow these steps:

1. Save a logo image file on your computer. Make sure that it conforms to the guidelines specified in Image File Tips (see page 14).

2. Log in as a user with the Administrator role.
3. Select Admin, Custom Settings, and click Themes.

   The Theme Settings page opens.
4. Click the Browse button to locate the image file to use in the custom theme.
5. Select the theme to which you want to apply the custom logo.

   Note: Select All Themes if you are not deploying multi-tenancy.
6. Click Save.

   The custom logo image is processed on the server. If it meets the image criteria, the change is saved to the theme.

   Images that do not meet the criteria cause a message showing the unmet requirements to appear. You can then modify the image and upload it again.
7. Edit the tenant (see page 132) to select the theme that you modified.

Image File Tips

The image file that you select for a custom theme must meet certain requirements so that it looks clear and fits into the available space. The best images to use in CA Performance Center custom themes conform to the following guidelines:

- The image is square. Use a 1:1 aspect ratio. If necessary, surround the logo with a square background.
- The image is in one of the following file formats:
  - .bmp
  - .gif
  - .png
  - .jpg
- (Optional) The image is transparent or white.
- (Optional) The image has a resolution setting of at least 300 dots per inch (DPI).
- Both CMYK and RGB color models are supported. However, CMYK color mode is a better choice for printer compatibility.

Display Settings

The Display Settings page lets you select preferences for the dashboards that you view in CA Performance Center.

View Suppression

By default, some dashboards contain data views that lack data. A message states, "No Data to Display".

A data view can be empty because of a configuration or connectivity issue. For views that report on technologies such as CBQoS, MPLS, or IP SLA, default views can be empty because the device that is selected for the view or page context is not configured to support that technology.

But in some cases, views are always empty because they lack a data source. Enable View Suppression to hide views when the required data source is not registered, or when a required technology is not configured.

Enabling the 'Suppress Views' option on the Display Settings page hides data views that lack a registered data source until that data source is registered. When the data source that populates a view is registered, that view is no longer hidden. Similar behavior applies to context tabs and custom menus. As long as a menu or tab has one view that is not suppressed, the custom menu or tab is still displayed.

Item Name Display Option

If your user account has the View Item Display Name or Name Alias role right, you can select how you want to identify items in dashboards and views. Display names are set by default. You can change this default setting to display item aliases instead.

Administrators can use a script to set aliases for monitored devices and interfaces (see page 16). When the Item Name Display option is set to Use Item Name Alias, the alias appears in the Inventory list of devices or interfaces.

More information:

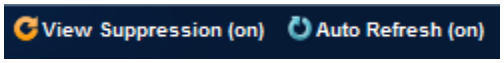
'No Data' Message in Views (see page 154)
Disable View Suppression (see page 16)
Set Item Aliases for Display in Dashboards and Views (see page 16)

Disable View Suppression

Enabling the 'Suppress Views' option on the Display Settings page hides data views that lack a registered data source until that data source is registered. When the data source that populates a view is registered, that view is no longer hidden.

View Suppression applies to views that are placed on dashboards by default. View Suppression does not hide views from administrators when they use the view categories to edit a dashboard.

The Suppress Views option is enabled by default. You can disable it for troubleshooting purposes, or to aid decision making when you are considering deploying another data source. When View Suppression is turned on, the View Suppression indicator is shown in the upper right of the page.



Follow these steps:

1. Log in to your user account. View Suppression is available to users with any role.
2. Select My Settings, Display Settings, and click the Display Settings menu item.

   The Display Settings page opens.
3. Select 'Display All Views' from the View Suppression menu.
4. Click Save.

   The View Suppression indicator disappears from the Infrastructure Overview page.

Note: When you enable View Suppression, you can also click the View Suppression indicator to access the Display Settings page.

Set Item Aliases for Display in Dashboards and Views

Users with the role right to View Item Display Name or Name Alias can select which name to display in their dashboards and views. Display names are set by default. You can change this default setting to display item aliases instead.

Administrators can set role rights.

Follow these steps:

1. Log in to your user account.
2. Select My Settings, Display Settings, and click the Display Settings menu item. This menu item is available to users who were given the "View Item Display Name or Name Alias" role right.

3. Select 'Use Item Name Alias' from the Item Name Display Option menu.

   Going forward, item aliases are displayed in dashboards and views.

   For the views that have column setting options, you can override the setting that you set in this procedure. For example, in Inventory views, you can select to display both the display names and aliases for items. A white arrow on the column lets you access a menu of table column options. Select Columns to enable and disable the metrics that were enabled for the table by default.

More information:

Set Alias Names For Multiple Monitored Devices (see page 163)
Set Alias Names For Interfaces and Components Across Multiple Monitored Devices (see page 166)

Managing Data Sources

Data sources are the supported products that provide performance and configuration data to CA Performance Center. Data source products that monitor, collect, and aggregate data can often function independently. However, once they are registered to an instance of CA Performance Center, they are known as data sources.

The data sources that are available to CA Performance Center depend on the compatible products that are installed and configured. You register data sources after installing CA Performance Center.

Occasionally, data sources require extra management. If you set up SSL encryption in your environment, it is required that you edit the data source connection parameters. A data source log (see page 24) is available to help you troubleshoot issues with data source connections.

Configuration data is automatically synchronized between CA Performance Center and registered data sources every 5 minutes. The status of global synchronization and a list of registered data sources are displayed on the Manage Data Sources page.

More information:

Register a Data Source (see page 25)
Edit a Data Source (see page 27)
Synchronize a Data Source (see page 23)

How Configuration Data from Data Sources Is Handled

The administrator for each data source can set some monitoring parameters and can create user accounts and other definitions. These parameters and definitions are shared with CA Performance Center and all other registered data sources after registration.

During registration, CA Performance Center imports user accounts, SNMP profiles, and other administrative data from the data sources. CA Performance Center resolves conflicts and eliminates duplication. At the next synchronization, it sends updated administrative data to all registered data sources.

The registration process includes a "binding" step that prevents further modifications to shared administrative data in individual data sources. As a result, the data source administrator can only modify shared monitoring parameters in CA Performance Center after registration.

Redundant Definitions in Data Sources

During registration, CA Performance Center imports user accounts and other configuration parameters from the data sources. Conflicts or duplicates are handled using the processes that are outlined in the following sections.

Redundant User Accounts

A user can have two different accounts with the same name in different data source products. The resulting user account retains the password of the first account that is synchronized. The unique role rights and permissions from the second or third account are added to the account as you register more data sources.

Multiple user accounts sometimes share a username in different data sources. Some account parameters differ. Manual editing is required in this situation. For example, assume that a user that is named Robert in CA Network Flow Analysis, and a different user, also named Robert, in CA Application Delivery Analysis. In this case, CA Performance Center creates one account that is named Robert. The role rights and permissions from both data sources are merged into the new account. To preserve the distinct role rights of the two accounts, create an account with a unique username.

Redundant SNMP Profiles

Registering a data source that contains SNMP profile definitions automatically adds the profiles to CA Performance Center. The profiles are distributed to the other registered data sources during the next synchronization.

When a data source is added, CA Performance Center minimizes duplication of SNMP profiles by comparing the following values to existing profiles:

- User (for SNMP v3)
- Community String (for SNMP v1 and v2)

If CA Performance Center detects duplicate parameters, CA Performance Center retains the most recent profile, as indicated by the timestamp.

CA Performance Center saves and appends a number to any duplicate Profile Name that is synchronized, but where the Community String values do not match. CA Performance Center the saves the new profile. For example, the first profile that is named Boston remains Boston. The second profile becomes Boston(1).

View a List of Data Sources

The Manage Data Sources page shows an inventory of registered data sources—the monitoring products that make data available for reporting.

The Manage Data Sources page lets you perform tasks that are associated with data sources. The page also shows the Global Synchronization Status—the last time that CA Performance Center contacted each data source for configuration and performance data.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Select Admin, Data Source Settings, and click Data Sources.

   The current list of data sources appears. If you have not registered any data sources, the list is empty.

   The following information is listed for each data source:

   Source Name

   Identifies the data source.

   Status

   Shows the status of the data source as it relates to CA Performance Center. Often indicates a synchronization phase. For more information, see Synchronization (see page 21).

   Last Polled On

   Indicates the time of the last successful synchronization. Normal synchronization occurs automatically every 5 minutes.

Source Type

Is the type of data source.

Version

Is the product version of the data source software.

3. Perform any action on this page by selecting a data source and clicking a button.

   Use the buttons at the bottom of the screen to perform the following tasks:

   Resync All

   Instructs the Device Manager service to initiate an incremental resynchronization with all data sources serially.

   Resync

   Initiates an immediate synchronization of the selected data source. Synchronization includes pushing all recently changed user, menu, and group settings to the data sources. Although synchronization occurs automatically every 5 minutes, this button starts it immediately. For more information, see Synchronization (see page 21).

   Test

   Runs a test to confirm that a new data source has been registered and is connected. A message provides test results.

   Log

   Opens the Data Source Log page for a selected data source. The data source log includes events that are associated with data sources and synchronization.

   Add

   Registers a new data source.

   Edit

   Lets you modify data source parameters.

   Delete

   Unregisters a selected data source. This action removes a selected data source from the list of data sources. For most data sources, removal releases product administration features that became read-only during registration. Once removed, a data source can be registered to another instance of CA Performance Center.

More information:

Register a Data Source (see page 25)
Edit a Data Source (see page 27)
Managing Data Sources (see page 17)
Synchronize a Data Source (see page 23)

Synchronization

CA Performance Center periodically synchronizes with registered data sources to send configuration information and retrieve data. The transmission ("push") phase incrementally replicates information to the data sources. Data sources receive group configuration, authentication settings, SNMP profiles, users, and roles. The information that is replicated to each database is filtered to include only items that the data source reported to CA Performance Center.

Once CA Performance Center has received data, it applies rules to associate metrics with managed items. Further changes to these definitions are prevented in the separate data source interfaces. The process of locking down data source administration is known as "binding." After the binding of definitions that are created in CA Performance Center, they are sent to the data sources.

Global synchronization refers to the automatic reception, processing, and application of information from the data sources. Synchronization occurs every 5 minutes and includes configuration and performance data from all registered data sources. It also takes place automatically each time a new SNMP profile is added.

Synchronization status is included in the table on the Manage Data Sources page. Failures and detailed statuses are included in the Data Source Log.

Full or Incremental Synchronization

A full synchronization occurs when a data source is first registered to CA Performance Center. A full synchronization involves a full database replication. CA Performance Center receives information about all managed items in that data source. This type of synchronization does not recur automatically on an ongoing basis, but you can manually initiate it if necessary.

When you change product configuration, it can be useful to initiate a manual synchronization. This action sends new definitions to a data source immediately instead of at the next (five-minute) synchronization interval. You can select whether to do a full or incremental data source synchronization when you initiate a manual synchronization.

Synchronization Status

If a *global synchronization* failure has occurred, administrators see a flashing icon at the top of the console page. To view more information about the failure, click the icon. The Manage Data Sources page opens. Review the information in the Global Synchronization Status section.

Important! If the 'Last Run Status' in the Global Synchronization Status section displays 'Failed,' contact CA Support.

If a *data source synchronizatio*n failure has occurred, administrators see a flashing icon at the top of the console page. To view more information about the failure, click the icon. The Manage Data Sources page opens. Review the information in the Data Sources section.

The Data Sources section displays the status of all registered data sources. The following messages describe possible data source status conditions:

Awaiting Poll

Indicates that the data source has never been contacted and is waiting for the Device Manager to poll it. The data source is polled quickly unless the Device Manager is busy performing another poll.

Awaiting Bind

Indicates that data has been retrieved ("pulled") from the data source. The data source is waiting for CA Performance Center to transmit ("push") configuration information and lock corresponding administrative features ("binding").

Available

Indicates that the data source is available for reporting. Registration has succeeded.

Polling

The Device Manager is in the process of polling the data source.

Registering

Indicates that the Device Manager is in the process of registering the data source.

Binding

Indicates that the device manager is in the process of locking the users, roles, and groups that are defined in the data source. Binding prevents further changes to configuration within the data source so that they match the definitions in CA Performance Center. Future modifications to these definitions are made in CA Performance Center, not in the data source.

Synchronizing

Indicates that the device manager is in the process of synchronizing with the data source by sending or receiving configuration information.

Polling Failure

Indicates that an unexpected failure occurred during polling. Click Log to view the Data Source Log.

Synchronization Failure

Indicates that a failure occurred during synchronization. Click Log to view the Data Source Log.

Registration Failure

A failure occurred during registration. Click Log to view the Data Source Log.

Bind Failure

Indicates that a failure occurred during the binding of users, groups, and roles. Click Log to view the Data Source Log.

Unable to Contact

Unable to contact the data source due to communication problems.

Version Incompatible

Indicates that the versions of CA Performance Center and the data source are not compatible. Contact CA Technical Support (see page 3) or check CA Support Online to find supported products.

Requires Upgrade

Indicates that the data source requires a software upgrade. Contact CA Technical Support.

Requires Registration

Indicates that the data source requires registration (waiting).

Requires Migration

Indicates that the data source requires migration (is waiting for the Device Manager).

Under Maintenance

Indicates that the data source is under maintenance.

Disabled

Indicates that the administrator has disabled the data source.

More information:

View the Data Source Log (see page 24)
Data Source Synchronization Failed (see page 150)

Synchronize a Data Source

CA Performance Center performs a regular global synchronization with all registered data sources every 5 minutes. You can also manually request a synchronization. Manual synchronization is useful for troubleshooting purposes, or as a means of immediately propagating a configuration change. For example, if you add a group, you can send the change down to the data source immediately by performing a manual synchronization.

When you initiate a manual synchronization, you can select a full or an incremental data source synchronization. You can synchronize a single data source, or multiple data sources.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Data Sources page (see page 19).

   The Manage Data Sources page displays the list of registered data sources.
3. Select the data source that you want to synchronize, and click Resync.

   The Resynchronize Data Source page opens.

   Note: By default, an incremental synchronization is performed. Only the records that are new from the last synchronization timestamp are included.
4. Select the 'Perform a full resynchronization' check box to perform a full resynchronization.

   A message asks you to confirm the action.
5. Click Resync to confirm the synchronization.

   CA Performance Center does the synchronization. A message appears only if any problems occur.

More information:

Data Source Synchronization Failed (see page 150)

View the Data Source Log

CA Performance Center logs information whenever errors occur. A separate log file is maintained for each service. These logs can be accessed from service-specific subdirectories under the CA\PerformanceCenter directory. For more information, see Logs (see page 147).

Synchronization occurs every 5 minutes. To avoid filling the log to capacity, only the initial synchronization and any failures that occur during subsequent full or incremental synchronization are logged. To determine when the last synchronization occurred, view the Last Polled On date on the Manage Data Sources page.

Use the Data Source Log to investigate suspected errors with the data source synchronization. You can drill down into event details from the Data Source Log page. You can use this information to troubleshoot issues that can occur with synchronization between databases.

Follow these steps:

1. Log in as a user with the Administrator role.

2. Navigate to the Manage Data Sources page (see page 19).

   The page displays the current list of registered data sources.

3. Select the data source whose log you want to view, and click Log.

   The Data Source Log page opens. The log is filtered to show only events that are related to synchronization for the selected data source.

More information:

Synchronize a Data Source (see page 23)
Synchronization (see page 21)
Data Source Synchronization Failed (see page 150)

Register a Data Source

Data sources must be registered before data can be made available in CA Performance Center dashboards. Registration takes place on the CA Performance Center Manage Data Sources page.

Note: For more information about data source version compatibility, see the Release Notes.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Data Sources page (see page 19).

   The current list of registered data sources appears on the Manage Data Sources page.

3. Click Add.

   The Add Data Source dialog opens.

4. Select the type of data source that you want to add from the Source Type list.

   Note: All CA products that can be registered as CA Performance Center data sources are shown in the Source Type list. The list is not filtered to show installed products.

5. Select the data source status. Select Disabled if you want to delay polling of this data source while still registering it.

   Note: No data from this data source is reported until you edit the data source to select the Enabled status. Views from this data source display a message stating, "No data to display".

6. Enter the Host Name of the data source.

   The hostname is typically the IP address or DNS hostname of the server where the database for this data source is installed.

   - For a Data Aggregator data source, supply the IP address or hostname of the host where the Data Aggregator component is installed.
   - For other data sources in a distributed configuration, supply the hostname of the management console.

7. Enter the port to use when contacting the data source. The port that you enter depends on the protocol that you select.

   For more information, see the *CA Single Sign-On User Guide*.

8. Select the protocol to use to contact the data source. Select **https** if your network is using SSL for communications. Verify that you have configured the system correctly before you select the **https** option.

   Note: SSL can be used for communications between CA Performance Center and the data source products. For more information, see the *CA Single Sign-On User Guide.*

9. (Optional) Enter a Display Name for the data source.

   By default, the data source type and the hostname are combined to create the display name. You can supply another name here. For example, instead of NetworkFlowAnalysis@xxx.x.x.xx, you can name the data source NetworkFlowAnalysis_NewYork.

10. (Optional) Clear the 'Web Console: Same as Data Source' check box to enable the Web Console options. You can supply another host name and port for the data source console.

    Note: The data source Web Console address is typically the same as the host name. Use this parameter in cases where network address translation is deployed.

11. (Optional) Select the Discover devices from other data sources check box. This option allows you to configure whether Data Aggregator automatically discovers devices that are synchronized with CA Performance Center by other data sources.

    Note: This option is available only when you select Data Aggregator as a data source.

12. Click Save to register the data source.

    The data sources that you have registered appear in the Data Source List.

More information:

Test Data Source Connections (see page 27)
Edit a Data Source (see page 27)

Test Data Source Connections

In most cases, the status indicates that data source registration has completed successfully. If the status indicates an error, use the test feature on the Manage Data Sources page.

The Test button initiates a test to confirm that a new data source is registered and connected correctly. The test checks for version compatibility and verifies that the data source is not registered with a different instance of the CA Performance Center software.

If the test fails, verify that the server name or IP address is accurate for the source type. For more information, see Data Source Test Failed (see page 152).

Edit a Data Source

You can edit registered data sources to change any of the parameters that you supplied. For example, you can change the display name that is associated with a data source.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Data Sources page (see page 19).

   The Manage Data Sources page displays the current list of registered data sources.
3. Select the data source that you want to modify, and click Edit.

   The Data Source Administration dialog opens.
4. Modify the settings as needed (see page 25).
5. (Optional) Select a data source, and click Test to verify that the data source is connected properly.

   If the connection fails, see Data Source Test Failed (see page 152) for more information.
6. Click Save.

More information:

Register a Data Source (see page 25)
Test Data Source Connections (see page 27)

Delete a Data Source

Selected administrators can delete a data source that is registered to CA Performance Center. A data source that you delete can be registered to another CA Performance Center instance. The removal process also unlocks data source administration.

Deleting a data source can have negative consequences. Only the administrators with the Delete Data Sources role right (see page 95) can delete a data source. This role right is not granted by default and must be assigned to the role as a separate step.

If View Suppression (see page 15) is enabled, views that are associated with a data source that you delete are suppressed. As a result, deleting a data source can cause menus and dashboards to become unavailable. To be displayed, a dashboard, context tab, or custom menu must contain at least one view whose data source is registered.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Roles page (see page 103).

   The page displays the current list of roles.
3. Select the Administrator role, and click Edit. The role right to Delete Data Sources is only available to this predefined role.

   The Edit Role Rights dialog opens.
4. Select Performance Center, and click Edit.

   The Edit Role Rights dialog lets you select individual access rights for this role.

   Assigned role rights are unavailable because they are read-only for this role.
5. Select Delete Data Sources.

   Click the right arrow to move it from the Available Rights list to the Selected Rights list.
6. Click OK. Then click Save to save your change to the role.
7. Navigate to the Manage Data Sources page (see page 19).

   The current list of registered data sources appears.
8. Select the data source that you want to delete (to unregister).

   The Delete button is activated.
9. Click Delete, and then click Yes to confirm the deletion.

   The data source is removed from the list.

SNMP Profiles

Many CA Performance Center data sources use SNMP to query the MIBs of managed items for performance information. *SNMP profiles* are definitions that contain the information necessary to enable secure queries of device MIBs using SNMP. These definitions provide SNMP parameters to data sources when needed while ensuring data security.

When you register a data source, any profiles that were created in the data source are added to CA Performance Center. The reverse also occurs: Profiles that are already established in CA Performance Center are sent back out and shared among all registered data sources. Naming conflicts are resolved. And any changes that are made to a profile are propagated to all registered data sources during synchronization.

Users with the Administrator role can create, edit, and delete SNMP profiles. Although all SNMP profiles are shared among data sources, they are specific to tenants. The Default Tenant Administrator sees a list of SNMP profiles that are associated with the Default Tenant (which is transparent in a single-tenant environment). In multi-tenant environments, each tenant administrator can only see the profiles for that tenant.

View the SNMP Profiles List

You can view a list of SNMP profiles that have already been defined. The list includes high-level information about the contents of each profile.

If no tenant definitions have been created, the definitions in the SNMP Profile List are shared among all registered data sources. The global administrator sees a list of SNMP profiles that are not explicitly associated with a tenant.

Note: Tenant administrators only see the items that are associated with their tenant.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Select Admin, System Settings, and click SNMP Profiles.

   The Manage SNMP Profiles page opens, and the current list of SNMP profiles appears.

   The following information is listed for each profile:

   Order

   Determines the order in which the secure information contained in an SNMP profile is used to try to query a selected device. If the query fails, the next profile is used, in priority order.

Profile Name

Defines a name for the SNMP profile. Profile names must be unique, cannot be duplicated across SNMP versions, and are not case-sensitive.

Port

Identifies the port that is used to make SNMP connections to devices associated with this profile.

Default: UDP 161.

SNMP Version

Specifies the version of SNMP that the profile uses. Because SNMPv1 and SNMPv2C are similar from a security standpoint, they share a single option. SNMPv3 is a separate option.

Authentication Protocol

(SNMPv3 Only) Specifies the authentication protocol to use when contacting devices associated with this profile. The following algorithms for authenticating SNMPv3 packets are supported:

- None (do not attempt authentication)
- MD5 (Message Digest 5)
- SHA (Secure Hash Algorithm)

Privacy Protocol

Identifies the encryption protocol that is used to contact associated devices, if any. Always 'None' if no authorization protocol is in use.

Use by Default

Indicates whether the information in this profile is used when not explicitly assigned to a device. If disabled, this profile is excluded from discovery in data sources that support the exclusion of profiles.

More information:

Add an SNMP Profile (see page 31)

Add an SNMP Profile

Administrators can create SNMP profiles to let registered data sources query devices for performance data. You can create these profiles for SNMPv1/v2c, or for SNMPv3.

If no tenant definitions have been created, SNMP profiles are shared among all data sources. However, SNMP profiles are specific to each tenant. The global administrator only sees a list of SNMP profiles associated with the Default Tenant. In multi-tenant environments, each tenant administrator can only see the profiles for that tenant.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage SNMP Profiles page (see page 29).

   The Manage SNMP Profiles page displays the current list of SNMP profiles.
3. Click New.

   The Add SNMP Profile dialog opens.
4. Complete the fields and change any default settings as required. Some fields apply only to SNMPv3.

   Profile Name

   Defines a name for the SNMP profile. Profile names must be unique, cannot be duplicated across SNMP versions, and are not case-sensitive.

   SNMP Version

   Specifies the version of SNMP that the profile uses. Because SNMPv1 and SNMPv2C are similar from a security standpoint, they share a single option. SNMPv3 is a separate option.

   Port

   Identifies the port that is used to make SNMP connections to devices associated with this profile.

   Note: Optional parameter for SNMPv1/v2C.

   Default: 161.

   User Name

   (SNMPv3 Only) Identifies the user for the profile, whose secret keys were used potentially to authenticate and encrypt the SNMPv3 packets. The User Name is a character string.

   Context Name

   (SNMPv3 Only) Identifies the collection of management information that is accessible by an SNMP entity. An octet string that is necessary for providing end-to-end identification and for retrieving data from an SNMPv3 agent.

Community Name

(SNMPv1/v2C Only) Defines a secure string that lets the data source query the MIB of the associated device. The community that you supply must provide read-only access to the device MIB.

Note: In the default SNMP profile, the community is 'public'.

Verify Community Name

Confirms the secure community string (name).

Authentication Protocol

(SNMPv3 Only) Specifies the authentication protocol to use when contacting devices associated with this profile. The following algorithms for authenticating SNMPv3 packets are supported:

- None (do not attempt authentication)
- MD5 (Message Digest 5)
- SHA (Secure Hash Algorithm)

Authentication Password

(SNMPv3 Only) Specifies the password for authentication using SNMPv3 and the selected authentication protocol.

Note: Supply an authentication password that is eight characters or more in length. Some data sources do not support authentication passwords or privacy passwords that fall below this minimum length. They treat the SNMP profile as invalid, and some data is not collected. Blank passwords are not supported for SNMP v3 profiles with MD5 or SHA as the Authentication Protocol.

Verify Authentication Password

Confirms the authentication password.

Privacy Protocol

(Optional) Specifies the encryption protocol to use for data flows sent to any devices or servers associated with this profile, as follows:

- None (do not encrypt communications)
- DES
- AES 128
- Triple DES

Note: The privacy protocol option is not enabled until authentication is enabled for this profile.

Privacy Password

Defines the password that is used when exchanging encryption keys. See the Note for a possible length requirement.

Verify Privacy Password

Defines the password used when exchanging encryption keys.

Use by default for new devices

Specifies whether the information in this profile is used by default. CA Performance Center uses this information to contact any new items that are discovered from monitored traffic. If it fails, the next profile in priority order is used. Disable this parameter to exclude a profile from discovery.

Note: This parameter does not apply to CA Infrastructure Management Data Aggregator data sources.

5. Click Save.
6. The Manage SNMP Profiles page appears. The new profile appears in the list.

   CA Performance Center automatically performs a global synchronization to send the profile information to all registered data sources.

More information:

Edit an SNMP Profile (see page 33)
Enable Administrators to View Data in Clear Text (see page 35)

Edit an SNMP Profile

Users with the required role rights can modify SNMP profiles to reflect changes to security settings.

Note: You cannot change the SNMP version of a profile once it has been created. The profile must be deleted and then recreated.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage SNMP Profiles page (see page 29).

   The page displays the current list of SNMP profiles.
3. Select a profile in the list, and click Edit.

   The Edit Profile dialog opens.
4. Modify the profile settings as needed (see page 31).

5. Click OK.

   Your changes are saved.

   The Manage SNMP Profiles page appears.

   CA Performance Center automatically performs a global synchronization to send the updated information to all registered data sources.

Change the Order of SNMP Profiles

Administrators can change the priority order of SNMP profiles to influence their selection in discovery and reporting. The Order parameter determines the order in which the secure information contained in an SNMP profile is used to try to query a selected device. If the query fails, the next profile is used, in priority order.

Tenant administrators can only see and manage the SNMP profiles available to the tenant domains with which they are associated.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage SNMP Profiles page (see page 29).

   The page displays the current list of SNMP profiles.
3. Select a profile in the list.
4. Click Move Up or Move Down to change the order in the list, or drag and drop a profile to the correct place.

   The SNMP Profile moves higher or lower in the list. The change in priority is saved to the database.

   Note: Move Up is disabled for the first item in the list; Move Down is disabled for the last item in the list.

Enable Administrators to View Data in Clear Text

By default, secure data is encrypted in the Add and Edit SNMP Profiles pages. As a result, it can be difficult to troubleshoot issues with SNMP polling.

You can let selected users see the Community that a profile is using, or the SNMPv3 authentication or privacy password, in clear text.

Note: The ability to view secure SNMP data in clear text is restricted to the predefined Administrator role.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Roles page (see page 103).

   The page displays the current list of roles.
3. Select the Administrator role, and click Edit. The role right to view SNMP Clear Text is only available to this predefined role.

   The Edit Role dialog opens.
4. Select Performance Center, and click Edit.

   The Edit Role Rights dialog lets you select individual access rights for this role.

   Assigned role rights are unavailable because they are read-only for this role.
5. Select the SNMP Clear Text role right.
6. Click the right arrow to move it from the Available Rights list to the Selected Rights list.
7. Click OK.

   The Edit Role dialog opens.
8. Click Save.

   The changes to the role are saved.

   By default, you have provided yourself with the ability to view secure SNMP data in clear text. The predefined Administrator role is assigned only to the global administrator by default. To let another user troubleshoot SNMP profiles and view security information in clear text, assign the Administrator role to another user account.

Delete an SNMP Profile

A host or tenant administrator can delete SNMP profiles when they are no longer needed.

Tenant administrators can only see and remove SNMP profiles for their own tenant.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage SNMP Profiles page (see page 29).

   The page displays the current list of SNMP profiles.
3. Select a profile, and click Delete.

   The Delete SNMP Profile dialog asks you to confirm the deletion.
4. Click Yes.

   The SNMP profile is deleted.

IP Domains

IP domains are logical groupings that identify data from different devices and networks. Monitoring by domain means that IP addresses with associated interfaces or applications that belong to separate customer networks are monitored separately. When combined with appropriate permissions, IP domains are monitored from a single console, but users view data only for the domains that they monitor.

IP domains were designed for use by service providers monitoring the networks of multiple discrete customers. Each customer account—each tenant—would therefore contain one or more IP domains.

Administrators and Designers can create custom dashboards to monitor activity on a specific domain or group of domains. Service provider administrators (that is, global administrators) can see data from all IP domains. But they can create user accounts that have permission to see data from a single customer domain.

Domain support is included with many CA data sources. Registration with CA Performance Center is required to enable it in the data sources.

About IP Domains

IP domains let you address potential IP address conflicts. Domain identifiers indicate that two managed items that otherwise appear as duplicate IP addresses are actually two *different* managed items. For example, a router with a single IP address could have multiple interfaces, each belonging to a different enterprise. The DNS identity of each interface would determine its IP domain. Data from items in the domain would be reported for a single tenant corresponding to the interface owner.

The domain dimension lets CA data sources function in a service-provider environment. The same software monitors multiple networks as separate entities. The domain lets data collectors associate managed items and data with the appropriate service provider customer, or *tenant*.

Domain monitoring is enabled for each data source as soon as it is registered. However, domain identifiers are not visible in the data sources until at least one custom IP domain definition has been created in CA Performance Center. The following managed item types are associated with the Default Domain once domain monitoring is enabled:

- Devices
- Interfaces and interface addresses
- Networks
- VoIP Locations

The data sources that monitor these item types report up a domain identifier and other properties during synchronization with CA Performance Center. A data source can associate an item with a domain by including a domain ID property. Any item whose domain ID is not reported is automatically placed in the Default Domain.

CA Performance Center users with the Administrator role can create custom IP domains. They are sent down to the data sources during synchronization, where they are available for use during data collection configuration. Domain definitions are shared among data sources that are registered to the same CA Performance Center instance.

In the Groups tree, the Domains group is contained within the Inventory group, which is itself a subgroup of the Tenant. The Domains group includes the Default Domain and any custom domains that you have created.

Items that are not assigned to a custom domain in a data source are associated with the Default Domain. This assignment is transparent to users who are not using custom IP domains to identify monitored traffic.

More information:

Set Up Tenant IP Domains (see page 136)
Associating Items with IP Domains (see page 44)
IP Domains (see page 36)
How IP Domains are Configured (see page 38)
Add an IP Domain (see page 40)

How IP Domains are Configured

IP domains function much like groups to contain managed items. Like groups, they are created in CA Performance Center, but the task of assigning items to domains is performed in the data sources.

IP domains are optional in a standard CA Performance Center installation. However, if you plan to deploy CA Performance Center in a multi-tenant environment, they are required.

The workflow for configuring IP domains is as follows:

1. Create tenants. For more information, see Creating and Managing Tenants (see page 125).
2. Create custom IP domains for each tenant. For more information, see Set Up Tenant IP Domains (see page 136).
3. Synchronize all data sources.

   You can either manually initiate a data source synchronization or wait for the next automatic synchronization to occur. For more information, see Synchronize a Data Source (see page 23).
4. Follow the instructions for each data source to associate items with the custom domains. For more information, see Associating Items with IP Domains (see page 44).

   Note: The data sources associate any items that are not specifically assigned to a custom IP domain with the Default Domain.
5. Synchronize all data sources in CA Performance Center. As soon as items are discovered, the domain containers within the Groups tree are populated with items.

View a List of IP Domains

IP domains are required for monitoring multiple tenants or environments with overlapping IP addresses. Each tenant requires at least one IP domain association.

When you begin creating tenants, access the list of IP domains and their parameters.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, Custom Settings, and click IP Domains.

   The Manage IP Domains page shows the current list of IP domains.

   If you have not created any custom IP domains, only the Default Domain appears in the list. This predefined domain has a 'null' setting for all parameters.

   Any custom domains that you have created have values for the following parameters:

   Name

   Identifies the domain.

   Description

   (Optional) Describes this domain namespace, such as naming the enterprise that owns it.

   DNS Settings

   (Optional) Select the DNS Settings checkbox to assign a primary and secondary IP address for the domain.

   Primary DNS Address

   Is the IP address of the primary name server for this domain.

   Primary DNS Port

   Is the port number that the primary name server uses.

   Secondary DNS Address

   Is the IP address of the secondary name server for this domain. Can be the same as the primary address.

   Secondary DNS Port

   Is the port number that the secondary name server uses.

Add an IP Domain

IP domains are required for monitoring multiple tenants or environments with overlapping IP addresses. Create custom IP domains in CA Performance Center so that items can be associated with domains and tenants by the data sources.

The Default Domain is automatically created. This domain includes any items that are not assigned to a custom domain in the data source.

When you have finished creating new domains, you can perform a manual synchronization to push the new domains to the data sources. Otherwise, synchronization automatically occurs approximately every 5 minutes.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage IP Domains page (see page 39).

   The page displays the current list of IP domains.
3. Click New.

   The IP Domains Administration dialog opens.
4. Supply information for the following parameters:

   Name

   Identifies the domain.

   Description

   (Optional) Describes this domain namespace, such as naming the enterprise that owns it.

   Device Name Alias

   Important! The following method of importing a CSV file of aliases is not the recommended method. Use the included script to set aliases (see page 163).

   Indicates the alias to use for a managed device. A device alias is a user-configured name that is applied to the associated managed item in CA Performance Center. Click Browse to navigate to and import a CSV file of aliases. The CSV file contains a comma-separated list of IP address-to-device alias mappings.

   Aliases that are associated with the primary IP address of a device take precedence over aliases that are associated with any secondary IP addresses. Look for the primary IP address in the Address column of the Inventory Devices list. We recommend always using the primary IP address of the device in the CSV file.

   For example:

   ```
   172.24.36.107,Austin Router
   ```

Browse to select the file and click Open.

If you include aliases for devices you are managing already, it can take up to 5 minutes to begin synchronizing these aliases with CA Performance Center.

Note: To remove an alias, import a CSV file that includes the IP address for the device and a *blank* alias column. To change an alias, modify the alias entry in the CSV file and reimport the file.

Interface Description Override

Important! The following method of importing a CSV file alternate interface descriptions is not the recommended method. Use the included script to set alternate descriptions (see page 166).

Indicates the alternate description to use for an interface. Interface descriptions appear in CA Performance Center already, but you can provide an alternate description. Click Browse to navigate to and import a CSV or TXT file of alternate descriptions. The file contains a comma-separated list of values that include the device IP address, interface name, interface description, and alternate interface description (alias) mappings.

For example:

```
172.24.36.107,ethernet_7,vmxnet3 Ethernet Adapter,Connection to Dallas
```

Note: Use the primary IP address of the associated device in the CSV or TXT file. Secondary IP addresses are not supported. Look for the primary IP address in the Address column of the Inventory Devices list.

Browse to select the file and click Open.

If you include alternate descriptions for interfaces you are managing already, it can take up to 5 minutes to begin synchronizing these descriptions with CA Performance Center.

Note: You *can* use the same alternate interface descriptions for more than one interface.

To remove an alternate description, import a CSV or TXT file that includes the IP address for the device, the interface name, the interface description, and a *blank* alias column. When you remove an alternate description, the original interface description reappears in CA Performance Center views.

Important! If you use a spreadsheet program to remove *all* of the alternate descriptions from a CSV file, include a column heading for the interface description override column in the imported file. If you do not include this column heading, the original interface descriptions will not reappear in CA Performance Center views.

To change a description, modify the alias entry in the CSV or TXT file and reimport the file.

DNS Settings

(Optional) Select the DNS Settings checkbox to assign a primary and secondary IP address for the domain.

Primary DNS Address

Is the IP address of the primary name server for this domain.

Primary DNS Port

Is the port number that the primary name server uses.

Secondary DNS Address

Is the IP address of the secondary name server for this domain. Can be the same as the primary address.

Secondary DNS Port

Is the port number that the secondary name server uses.

5. Click Save.

   The new IP domain appears in the list.

6. Repeat the steps as required to add more IP domains.

More information:

Device Name Display (see page 160)

More information:

Synchronize a Data Source (see page 23)
About IP Domains (see page 37)
Add an IP Domain (see page 40)

Edit an IP Domain

You can edit the custom IP domains that you have created. The changes are propagated to all registered data sources at the next synchronization.

The Default Domain cannot be edited. It must remain sufficiently generic to include all managed items that are not assigned to a custom domain by the data sources.

When you have finished editing domain definitions, you can force a synchronization to push the changes to the data sources. Otherwise, synchronization automatically occurs approximately every 5 minutes.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage IP Domains page (see page 39).

   The page displays the current list of IP domains.
3. Click Edit.

   The IP Domains Administration dialog opens.
4. Modify the parameters as needed (see page 40).
5. Click Save.

   Your changes to the IP domain are saved and are reflected in the IP Domain List.

   Changes to IP domains are not applied to managed items until synchronization has occurred. Within each tenant, managed items already reported remain unchanged in historical data views.

Delete an IP Domain

Like the associations between performance statistics and managed items, IP domain associations are stored along with items in the database on each data source console. As a result, domains cannot simply be deleted from CA Performance Center.

If you delete a domain, it can be marked as inactive in the data source. An inactive domain is not exposed in views that display new data. But if you unregister (remove) the data source and register it again later, the data source sends the domain information back up to CA Performance Center at the first synchronization. Managed items in the data source database retain the domain association.

For some data sources, deleting a domain causes data loss, such as polled device information and history. Reinstallation steps are required in such cases. Proceed with caution when you want to delete an IP domain.

In most cases, the workflow outlined in the following procedure is recommended:

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage IP Domains page (see page 39).

   The page displays the current list of IP domains.

3. Select the IP domain that you want to delete.
4. Click Delete, and click Yes to confirm the deletion.

   The domain is deleted from the list of IP domains.
5. Edit the data collector for each affected data source to change the domain assignment it is using, replacing the deleted domain.

   Note: We recommend selecting another custom domain for the affected data collectors. Otherwise, they will associate items with the Default Domain.

   Any data that was previously collected and associated with the deleted domain remains associated with it and is displayed as such in historical views.

Associating Items with IP Domains

Although you create IP domains in CA Performance Center, the data sources associate items with domains. Each data source assigns domain IDs to the items it discovers from monitoring data traffic. Therefore, no managed items receive domain associations until the data source administrators set collection parameters.

A tenant only contains the items in its own tenant IP domains. Therefore, tenant dashboards are empty until:

- An IP domain is associated with the tenant.
- Synchronization has occurred between CA Performance Center and the data sources.
- The data sources have been configured to associate managed items with IP domains.

We recommend creating IP domains as soon as you create each tenant. Follow the recommended workflow described in How IP Domains Are Configured (see page 38).

Knowledge of IP address schemes for all networks in all monitored enterprise systems is required to verify that domains are populated correctly.

How to Populate IP Domains with CA Infrastructure Management Data Aggregator

Each CA Infrastructure Management Data Collector host associates managed items with a single IP domain. To enable multi-tenant deployments, assign an IP domain to each Data Collector as soon as you have installed the software.

Before you install a Data Collector, use the CA Performance Center Admin interface to create the tenants and IP domains that you require.

Note: A single IP domain can be associated with multiple Data Collector components. However, only one IP domain can be assigned to each Data Collector component.

Follow these steps:

1. Log in to CA Performance Center as a user with the Administrator role (a global administrator).
2. Create a tenant.
3. Administer the tenant, or log in as the tenant administrator.
4. Create the IP domain in CA Performance Center.

   The new IP domain appears in the IP Domain list, which is scoped to the current tenant. Other tenant users cannot see items in this IP domain.
5. Install Data Aggregator components.
6. Synchronize the Data Aggregator component with CA Performance Center.
7. Install the Data Collector component.

   Note: For more information about how to install the CA Infrastructure Management Data Aggregator components, see the *CA Infrastructure Management Data Aggregator Installation Guide*.

   You are asked whether to associate the Data Collector with the Default Tenant. We recommend making this association if you are not deploying multi-tenancy.
8. Select Admin, Data Source Settings, and click a Data Aggregator data source.
9. Click Data Collectors in the System Status menu.

   The Data Collector List page opens, displaying a list of available Data Collector installations.
10. Select an IP domain and a tenant for each Data Collector in the list, and click Assign.

    Note: If you are not deploying multi-tenancy, keep the Default Tenant assignment.
11. Create a Discovery profile that is associated with each IP domain that you have configured.

    Note: For more information about Discovery, see the *CA Infrastructure Management Data Aggregator Administrator Guide*.

Change the Domain of Interfaces and CVIs

Interfaces and CVIs inherit their initial tenant-domain setting from the parent router and Harvester. The setting is inherited when the parent Harvester is added and the router and interfaces first become active. If the Harvester is not associated with a custom domain, the routers and interfaces are assigned to the Default Domain as they become active.

You can edit the settings for interfaces and CVIs to associate them with any tenant and domain at any time. The setting does not have to match the parent router or Harvester.

Changing this setting can affect which operators have access to the interface's data. The setting does not affect which SNMP profiles are used for polling. The router tenant determines the set of SNMP profiles for polling.

Follow these steps:

1. Open the Active Interfaces page:
   a. Select Administration from the NFA console menu.

      The Administration page opens.

   b. Select Interfaces: Physical & Virtual from the Administration menu.

      The Active Interfaces page opens.
2. Locate and select the check box next to one or more interfaces that you want to associate with a tenant and domain.
   - To search for parent routers, interfaces, or CVIs, enter all or part of a router IP address, a router or interface name, or an interface description in the Search field, and then click Search. Expand the router details.
   - To navigate to an interface or CVI manually, go to the page that contains the parent router and click the arrow next to the router name. The router details expand to show the interfaces and CVIs.
3. Click Edit.

   The editing dialog opens. The Domain selection list is included in the dialog only if multiple domains exist.
4. Select a tenant / domain option from the Domain list.
5. Click Save.

   The dialog closes. The changes are shown on the Active Interfaces page.

Note: You can also change the tenant-domain setting for Harvesters and routers.

Populating IP Domains with CA Application Delivery Analysis

CA Application Delivery Analysis can observe duplicate IP traffic. Such traffic occurs in a managed service provider (MSP) environment. The provider can host an application on a single server for multiple customers whose environments contain overlapping client IP addresses.

You enable CA Application Delivery Analysis to identify separate IP traffic during data collection setup. As you verify and modify data collection parameters, assign the same IP domain to the appropriate:

- Monitor feeds.
- Client networks.
- Servers or server subnets.

With the same IP domain assignments for these feeds, CA Application Delivery Analysis reports on the application traffic between a client and a server by domain.

Applications are domain-independent. Therefore, you are not required to define the same application twice, such as Exchange Company A and Exchange Company B, to enable CA Application Delivery Analysis to report on application performance across domains. However, to set different thresholds for application performance, performance OLAs, and availability OLAs, create an application for each IP domain.

If you do not need to separate duplicate IP traffic, you can use the DNS settings in the Default Domain to query DNS and resolve the hostname of a CA Application Delivery Analysis server. Otherwise, CA Application Delivery Analysis uses the monitor feed that is assigned to the server to resolve the hostname.

View a List of Domains in CA Application Delivery Analysis

You can view a list of domain definitions and current domain associations in the Administration section of the CA Application Delivery Analysis management console.

Note: Any items that are not assigned to a specific domain in a data source are included in the Default Domains group. In the data source, they appear to be associated with the Default Domain.

Follow these steps:

1. Click the Administration tab in the management console.
2. Click Data Monitoring, Domains in the Show Me menu.

   The Domains page opens.
3. (Optional) View the DNS settings for a domain by clicking the magnifying glass symbol in the View column.

   The Domain Properties page opens.

4. Verify the properties.
5. Click OK when you have finished.

   You return to the Domains page.

Assign a Domain to a Monitor Feed

You can instruct each Standard Monitor to associate the items it monitors with a custom domain as part of CA Application Delivery Analysis collection device setup.

Note: Any managed items that are not associated with a custom IP domain by a data source are associated with the Default Domain. This assignment is transparent to users who are not deploying custom IP domains.

Follow these steps:

1. Click the Administration tab in the management console.
2. Click Data Monitoring, Monitoring Devices in the Show Me menu.

   The CA Application Delivery Analysis Monitors list page opens.
3. Click Edit to edit a multifunction monitoring device, such as a Standard or Multi-Port Monitor.

   The Monitor Properties page opens.
4. Scroll down to the Monitor Feeds list.
5. Click to edit a monitor feed.
6. Select a custom IP domain.
7. Click Update.

   All items detected by this monitor feed are automatically associated with the selected IP domain.

Assign a Domain to a Client Network

After you add a client network, you cannot change its IP domain association. If you need to change the assigned IP domain, you must delete the network and then add it to the correct domain.

Note: Any managed items that are not associated with a custom IP domain by a data source are associated with the Default Domain. This assignment is transparent to users who are not deploying custom IP domains.

Follow these steps:

1. Click the Administration tab in the management console.
2. Click Data Monitoring, Networks in the Show Me menu.

   The Networks List page opens.

3. Select the IP domain from the list.
4. Click Add Network.
5. Enter the required information to add the network.
6. Click OK.

Assign a Domain to a Server or Server Subnet

After you add a server or server subnet, you cannot change its IP domain. If you add a server or server subnet to the wrong IP domain, you must delete it and then add it to the correct domain.

Note: Any managed items that are not associated with a custom IP domain by a data source are associated with the Default Domain. This assignment is transparent to users who are not deploying custom IP domains.

Follow these steps:

1. Click the Administration tab in the management console.
2. Click Data Monitoring, Servers in the Show Me menu.

   The Server Subnet List and Server List page opens.
3. Select the IP domain from the list.
4. Supply the information to add the Server or Server Subnet.
5. Click OK.

Populate IP Domains with CA Unified Communications Monitor

In the CA Unified Communications Monitor management console, you can instruct collectors to associate the items they discover with custom domains in CA Performance Center. The act of creating a single custom domain in CA Performance Center enables domain associations for Locations, voice gateways, and call servers in any registered data sources.

Items appear with domain designations as soon as they are discovered from call traffic. Items discovered previously do not receive retroactive associations.

Locations are automatically associated with IP domains by the subnets that they contain. To preserve the flow of data collection and the appropriate association of data with IP domains, take care when moving Locations to new IP domains. Follow the procedure provided in the CA Unified Communications Monitor online Help to change IP domain assignments.

Note: Any managed items that are not associated with a custom IP domain by a data source are associated with the Default Domain. This assignment is transparent to users who are not deploying custom IP domains.

Instruct collectors to associate items with custom IP domains.

Follow these steps:

1. Click Administration, Data Collection, Collectors.
2. Edit each collector to select its domain for the IP Domain parameter.
3. Reload the collectors to send them the domain information.

   Domains are populated with managed items after the next product synchronization.

Notifications

Notifications can be configured for events coming from a data source to the Event Manager. The incoming events are evaluated against the conditions that you configure for the notification criteria. Only when the criteria are met does Event Manager take a notification action. If an event does not trigger a notification, the event can still be displayed in the Event List.

Note: For information about which data sources are supported for notifications, see the *CA Performance Center Readme*.

A user only configures and receives notifications for events for an item in a group to which the user has access.

Important! Create an SNMP profile with the outgoing trap port (typically 162) before creating the notification.

Consider the following information:

- Notifications are user-specific; users cannot see the notifications of others.
- The action to delete event notifications does not affect the actual or future events.

The following notification types are available in the Create/Edit Notifications wizard:

Trap

Sends trap notifications to fault or network management system (NMS) in your environment, such as CA Spectrum. Supports multiple destinations. The first destination is required.

Two MIB choices are available in the Notifications wizard to provide compatibility for existing customers.

Note: The trap receivers must be preconfigured to receive traps. Each destination can have its own configuration regarding SNMP community and IPV4 destination. For more information about trap formats, see the corresponding NMS documentation for your trap receiver.

Supported roles: Users with the Administrator role (global administrators) can configure trap notifications. Administrators must also have product privileges to a data source that creates events.

Email

Sends email notifications to one or more recipients when an event is raised or cleared. Provides a link in the email to the context page for the device or component that triggered the alarm.

Supported roles: Users with the Create Notifications role right and users with the Administrator role and product permission can configure email notifications. However, the Administrator role must first specify an SMTP server.

Administrators can view, create, or delete notifications from the Admin, Notifications menu in the CA Performance Center user interface. The Notifications option only displays when Event Manager is enabled and in a synchronized state of Available.

Note: As a Default Tenant Administrator, you can create a notification for a tenant administrator or tenant user by working in a real user context. Log in as a tenant administrator or tenant user. Alternatively, the Default Tenant administrator can administer the tenant and then proxy to the user to create a tenant-scoped notification.

Alternatively, administrators can use the Event Manager API. Access the self-documenting interface on the Event Manager host using this URL: http://*hostname:*8281/EventManager/webservice/notifications/documentation.

Users can create email notifications from the My Settings, Notifications menu.

More Information:

nhLiveAlarm Format Usage for Traps (see page 53)
EventManager Format Usage for Traps (see page 52)

EventManager Format Usage for Traps

The EventManager MIB is supported for trap notifications. If needed, the MIB files can be found in:

InstallLocation/PerformanceCenter/PC/webapps/pc/mibs/netqos-em-mib

InstallLocation

Is the directory where CA Performance Center was installed.

When the EventManager format choice is selected, the trap will be sent out with the following variables:

netQosEventId

Specifies an identifier that Event Manager assigned to the event.

netQoSEventType

Specifies the type of event.

netQoSEventCategory

Categorizes the event.

Values: 0 Unknown, 1 Fault, 2 Config, 3 Accounting, 4 Performance, 5 Security

netQoSEventSeverity

Specifies the severity of the event.

Values: 0 Normal, 1 Unknown, 2 Minor, 3 Major, 4 Critical, 5 Unavailable

netQoSEventDescription

Describes the event.

netQoSEventState

Specifies the current state of the event. Each state has its own notification.

Values: 0 opened, 1 acknowledged, 2 closed, 3 cleared

netQoSEventOpenTime

Specifies the UTC timestamp (from the eventState timestamp).

netQoSEventMapURL

No value is available. The "" string will be sent.

netQoSEventDetailsURL

No value is available. The "" string will be sent.

netQoSEventAssociatedItemURL

Specifies the URL to the item web page.

netQoSEventItemName

Specifies the item name. There is one notification per item.

Maximum length: 127 bytes

netQoSEventItemType

Specifies the item type.

Maximum length: 32 bytes

netQoSEventItemSubtype

Specifies the item subtype.

Maximum length: 32 bytes

netQoSEventItemIpAddress

Specifies an IP address for the item or an empty string.

netQoSEventPropertyName

Specifies one name set for each property. There will be a PropertyName for each property in the event. (The properties will vary by the event type.)

Maximum length: 128 bytes

netQoSEventPropertyValue

Specifies the property value for the event. There will be a PropertyValue for each property in the event. (The properties will vary by the event type.)

nhLiveAlarm Format Usage for Traps

The nhLiveAlarm MIB is supported for trap notifications. If needed, the MIB files can be found in:

InstallLocation/PerformanceCenter/PC/webapps/pc/mibs/concord-diagmon.mib

InstallLocation

Is the directory where CA Performance Center was installed.

When using the nhLiveAlarm format for trap notifications, be aware of the following restrictions. Many of the variable values described by the CA eHealth trap MIB have changed from integrations with earlier versions of NetQoS Performance Center.

nhServerIp

No value is available. The "" string will be sent.

nhServerName

No value is available. The "" string will be sent.

nhServerPort

No value is available. The "" string will be sent.

nhElementIp

Specifies the IP address of the item or "" if no IP address exists.

nhElementName

Specifies the item name.

nhElementId

Specifies the item CA Performance Center ID (global ID).

nhStartTime

Specifies the timestamp from the event.

nhDisplayStr

Specifies the value for the MaxThresholdValue variable from the event.

nhGroup

No value is available. The "" string will be sent.

nhGroupList

No value is available. The "" string will be sent.

nhExceptionType

No value is available. The "" string will be sent.

nhVariable

Specifies variables in the event profile rule.

nhSeverity

Specifies the severity of the event.

nhOpenViewSeverity

No value is available. The "" string will be sent.

nhProfile

Specifies the event profile name.

nhExceptionId

Specifies the event ID.

nhTechType

No value is available. The "" string will be sent.

nhEventCarrier

No value is available. The "" string will be sent.

nhElementAlias

No value is available. The "" string will be sent.

nhComponent

No value is available. The "" string will be sent.

nhDescription

Contains the event description.

nhAlarmOccurId

Specifies the alarm ID.

profileId

Specifies the event profile ID.

nhElementBaseType

Specifies the item type.

About Business Hours

At certain times of the day and on certain days of the week, business activities occur in greater or in reduced volumes. The resulting infrastructure usage patterns are regular and predictable. During the times of increased business activity, optimal network and server performance is critically important. But by default, CA Performance Center dashboards do not differentiate reported data according to its impact on business activities.

To help CA Infrastructure Management operators focus on the data with the greatest impact on the business, the administrator can associate business-hours definitions with site groups. Site groups let you organize managed networks and devices geographically. Each site group can have one associated set of business hours and one time zone. To help IT operators and engineers manage the multiple time zones in your enterprise and prioritize troubleshooting activities, deploy site groups with associated business hours.

To create a strategic plan, deploy business hours with the following settings:

- site groups that contain managed items in geographical proximity
- user accounts with accurate time zones for the associated operator and locale
- business-hours definitions that capture times of increased business activity throughout the enterprise

Each business-hours definition includes both times of day and days of the week. Select the hours and days that reflect periods of increased commercial activity. We recommend creating these definitions for every distinct location in your enterprise.

Manage Business Hour Definitions

The Manage Business Hours Definitions page shows a list of the business-hour definitions that you can associate with site groups. Options on this page let you perform tasks that are associated with business-hour definitions.

We recommend adding business-hour definitions before you create site groups. You can then assign business hours during site group creation.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, Custom Settings, and click Business Hours.

   The Manage Business Hours page displays the current list of definitions. If you have not created any business-hour definitions, the list is empty.

   Note: Tenant administrators only see the items that are associated with their tenant.

   The following information is listed for each definition:

   Name

   Is the name of the business-hour definition. Appears in the list to identify this definition when you associate business hours with site groups.

   Description

   Describes the definition to help you identify it.
3. Perform any action on this page by selecting a definition in the list and clicking a button.

   View Sites

   Shows the site groups that have this business-hour assignment, and lets you change the assignment if desired.

More information:

Create a Site Group (see page 75)
About Business Hours (see page 55)
Create Business-Hour Definitions (see page 57)
Edit and Associate Business Hours (see page 58)

Create Business-Hour Definitions

Create business-hour definitions that you can then associate with site groups. Each definition includes both times of day and days of the week. Select the hours and days that reflect periods of increased commercial activity. We recommend creating these definitions for every distinct location in your enterprise.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, Custom Settings, and click Business Hours.

   The Manage Business Hours Definitions page opens.
3. Click New.

   The Add Business Hour dialog opens.
4. Supply a name for the business-hour definition.
5. (Optional) Supply a description of this definition.

   Note: The name appears in the list to identify this definition when you associate business hours with site groups. The description only appears in the list of definitions on the Manage Business Hours Definitions page.
6. Select the check boxes next to the days of the week that you want to include in this definition.

   For example, select Mon, Tue, Wed, Thu, and Fri to create a definition that spans a typical work week in the United States.

   Note: Assigning multiple business-hour definitions to a single site is not supported. Similarly, selecting a start time and end time that span more than 24 hours is not supported.
7. Use the first dropdown on the left to select the start time for these business hours.

   Use the second dropdown to select the end time. Half-hour increments are not supported.

   Business hours have no effect until they are associated with site groups.
8. (Optional) Associate business hours with site groups from the same dialog if you have already created site groups:

   a. Click Select Site Groups to Associate.

      The Select Site Groups to Associate dialog opens.

b. Select a site group in the Available Sites list.

c. Click the right arrow button to move the group to the Selected Sites list.

Note: You can also associate business hours and time zones with site groups when you create site groups (see page 75).

9. Click OK.

   You return to the Add Business Hours dialog.

10. Click Save.

    The business-hour definition appears in the list.

Edit and Associate Business Hours

The Manage Business Hour Definitions page lets you create and modify business-hour definitions. You can also associate business hours with site groups on this page.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, Custom Settings, and click Business Hours.

   The Manage Business Hour Definitions page displays the current list of definitions.

3. (Optional) Check the current usage of the business-hour definition that you want to modify, and change it, if desired. Take the following steps:

   a. Select the definition.

   b. Click View Sites to open the View Sites for Selected Business Hour Definition dialog.

      Any sites with this business-hour association are shown in the list of Selected Sites.

   c. (Optional) Select a new site group in the Available Sites list.

      Note: Custom groups cannot be selected. The cursor is only enabled for selection when you hover over site groups in the tree.

   d. Click the right arrow button to move it to the Selected Sites list.

   e. (Optional) Use the same technique to delete a business-hour association: select a site group, and use the left arrow to remove it from the Selected Sites list.

4. Select a definition that you want to edit.
5. Click Edit.

   The Edit Business Hours Definition dialog opens.

6. Modify business hour settings (see page 57) as required.
7. Click Save.

   The changes to the definition are saved.

Delete a Business-Hour Definition

When a business-hour definition is no longer being used, you can delete it. Deleting a business-hour definition that is associated with a site group also removes the association.

You can also remove the association of business hours with site groups in a separate procedure. When you remove only the association, the definition itself is still available to be assigned to another site. Click View Sites on the Manage Business Hour Definitions page to remove an association.

When you delete a business-hour definition or its association with a site group, the site group loses business-hour filtering in data views. In the context pages for the items that belong to this site group, the Details tab indicates that the items are "not a member of a site group that includes time settings."

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Business Hour Definitions page (see page 56).

   The page displays the current list of business-hour definitions.
3. Select the definition that you want to delete, and click Delete.

   The Delete Business-Hour Definition dialog opens.
4. Click Yes to confirm the deletion.

   The definition is deleted and no longer appears in the list. Any site groups that had this business-hour assignment now lack business-hour filtering. The managed items that these site groups contained also lack this filtering option but are not otherwise affected.

Chapter 3: Creating and Managing Groups

This section contains the following topics:

Creating and Managing Groups

The administrator can create a custom group structure to organize managed items in CA Performance Center. Groups act like filters to organize related items and make reported data more useful. For example, a group can represent a physical location, a device and its interfaces, or a group of similar devices. Custom groups let operators view the items that they can monitor, while limiting their access to the selected data.

Properly configured groups can prevent CA Performance Center operators from viewing selected data for security reasons. The administrator can selectively grant user access to data that falls within their area of responsibility. Groups can also facilitate performance monitoring, reporting, and troubleshooting.

Tenants include special types of system groups to maintain separation among customer deployments. Tenants can also contain entire custom grouping structures.

More information:

Create a Custom Group (see page 73)
Types of Groups (see page 62)
Custom Groups (see page 65)
Groups for Multi-Tenant Deployments (see page 68)

Types of Groups

Groups are organized into a hierarchical tree structure. The Groups tree helps you define relationships, policies, and dependencies among services, devices, applications, locations, and users within your organization. The following list summarizes the types of groups in the Groups tree:

System Groups 

Are read-only groups automatically created by CA Performance Center based on information from data sources. These groups cannot be edited (as indicated by the "lock" symbol). But they can be viewed, applied as permission groups to user accounts, or copied to custom or site groups.

Custom Groups 

Create hierarchical levels and organize items into logical relationships within the Groups tree. Custom groups at the top level of the Groups tree typically represent geographical, topological, or functional divisions within your organization. Lower-level custom groups (or subgroups) typically represent managed item types, such as devices, services, or applications. Or these subgroups can represent the job functions of IT staff.

Only administrators can create and edit custom groups. They filter the data in CA Performance Center dashboards and views. The group context for a dashboard or view determines the data that is presented.

Site Groups 

Are special custom groups based on sites, such as branch offices, or on physical locations, such as regions or cities. Site groups let you create navigation functions within CA Performance Center dashboards to present views across all sites. They include a Time Zone and a Business Hours parameter to let you see prioritized data from business-critical times of day.

Site groups also provide a granular context to apply to dashboards. For example, after you create a site group for each of your sites, a single dashboard can report on each site individually. We strongly recommend creating a site group for each data center within your enterprise and for other major infrastructure locations.

Group References

Are read-only copies of system or custom groups. When you copy a group to another location in the Groups tree, a group reference appears. User permissions can be allocated using group references. Using references lets you create a group structure once, and then copy that structure to other parts of the Groups tree. Changes to group references can only be made to the original custom group, but they are propagated to all reference locations.

Select a group reference to access a link to the original group. Clicking the link expands the node in the Groups tree and opens the Properties tab for the original group.

System Groups

When you register a data source, system groups are automatically created to organize the items in the database. Use system groups to build custom groups and manage the items in your inventory.

System groups cannot be edited; however, you can add them to custom groups as subgroups and can assign them to user accounts as permission groups. A lock icon indicates their read-only status: .

The following system group is automatically included in the Groups tree:

Inventory

Includes all managed items that are discovered by all registered data sources. Organizes data sources, IP domains, and managed items in subgroups.

If you have registered a CA Infrastructure Management Data Aggregator data source, the following system group appears at the same level in the Groups tree:

Collections 

Represents the collections of managed items. Collections are groupings of items that are monitored using the rules that are specified in CA Infrastructure Management monitoring profiles. The "factory" collections are not visible in the Groups tree.

This group lets you create custom CA Infrastructure Management collections. Any subgroup that you add to the Collections group is synchronized to the CA Infrastructure Management Data Aggregator as a collection.

Special groups for multi-tenant deployments also appear after you create at least one custom tenant. For more information, see Groups for Multi-Tenant Deployments (see page 68).

The Inventory group contains its own system subgroups to organize managed items by their type. Multiple data sources share some system subgroups, such as the Routers group. Other subgroups are specific to a single data source.

The following system groups appear when you expand the Inventory node:

All Items 

Includes subgroups of managed items, which are categorized by type.

Data Sources 

Includes all data sources that are registered with CA Performance Center. Each data source has a dedicated group under this node.

Note: A data source typically has its own system subgroups, which you can see when you expand the data source group.

IP Domains 

Includes all of the custom IP domains created by the administrator. Also includes the Default Domain, which contains all items that are not explicitly assigned to a custom domain. For more information, see IP Domains (see page 36).

The All Items subgroup of the Inventory group contains the following system subgroups of items. You can click any of these groups to view their actual membership on the Items tab:

All Pingable Devices 

Includes all discovered devices that cannot be contacted using SNMP.

ESX Hosts

Includes all VMware servers that host virtual machines.

Interfaces

Includes router and switch interfaces from all data sources.

Routers

Includes all routers from all data sources.

Servers

Includes all servers from all data sources.

CA Application Delivery Analysis Networks

Includes all networks that CA Application Delivery Analysis has observed. A CA Application Delivery Analysis network consists of an IP address and mask.

Switches

Includes switches from all data sources.

Virtual Machines

Includes all virtual machines running on all ESX servers.

Custom Groups

Custom groups are a key component in a strategy to monitor and manage your system. Creating custom groups lets you organize data and assign operator permissions to access data to each CA Performance Center.

The term *permission groups* describes groups that have been selected to act as high-level permissions. Permission groups are assigned to user accounts, and they precisely determine the items and data that each operator can view. Create custom groups that you can assign as permission groups or as administered groups.

You can create groups by using system groups as building blocks. You can use group rules to add items to groups automatically, as they are discovered during monitoring. Setting up rules makes it easier to populate and maintain groups. You can also populate custom groups by adding specific items manually, such as routers or interfaces that are logically or geographically related.

To create narrower sets of accessible data, add subgroups to permission groups. Using subgroups to allocate permissions helps users to narrow their focus, and to investigate and monitor possible areas of concern. You can assign the subgroups to user accounts that need a narrow focus, and can assign the higher-level group containers to those that need a broader scope.

The main consideration when creating any custom groups is how they can be used to give users access to the data they want to view. You can create custom groups to address the job function of an individual, or to group similar items together.

Site groups are custom groups that are based on physical locations, such as a city, region, office, or campus. Typically, site groups contain items and subgroups of items that are grouped by location. Adding site groups to other custom groups in your tree structure allows you to build geographically and logically organized reports. Site groups enable business-hour filtering of dashboard views.

Similar to other custom groups, site groups can contain subgroups. When building site groups, you can, for example, start with a region and add subgroups containing cities. You can then add more subgroups to contain buildings within each city.

More information:

Create a Custom Group (see page 73)
Types of Groups (see page 62)
Create a Site Group (see page 75)

Grouping Best Practices

Creating custom groups to manage your networks and devices, or those of your customers, is a recommended best practice. Custom groups can be based on job function, on sites within an enterprise, or on more granular categories, such as related devices or device interfaces. The Groups feature includes features to let you create multiple structures. You can use individual groups multiple times, in various places in the Groups tree.

A recommended best practice for creating useful groups is to create a "master" group structure that is based on the infrastructure topology of your enterprise. You can then use these groups as references in other custom group structures.

The following example shows a hierarchical group structure for an enterprise network:

Groups for Multi-Tenant Deployments

When the global administrator (the administrator for the Default Tenant) creates at least one tenant, features to support multi-tenancy are enabled. "Multi-tenant deployments" consist of multiple discrete enterprises with potentially overlapping IP addresses. More groups appear in the Groups tree to let the administrator organize tenant inventories and allocate permissions:

Defined Tenants

Includes all tenants. Tenants are used with IP domains to monitor separate customer environments with a single CA Performance Center instance. Each tenant can contain multiple subgroups of items that are not shared among tenants.

Tenant administrators can create custom groups within their tenant. For the global administrator, tenant groups appear under the Tenant node in the Groups tree.

Service Provider Global Groups

Contains groups of items that help the global administrator manage tenant environments. These groups let the administrator visualize and organize shared items–any items that are not explicitly associated with a tenant IP domain.

The groups that allocate access to data from shared items appear under each tenant. See "Service Provider Defined Groups."

When you expand the top-level Inventory group, the following group appears in a multi-tenant deployment:

Domains

Includes all of the custom IP domains that are used to associate managed items with tenants. Also includes the Default Domain, which contains all items that are not explicitly assigned to a custom domain. For more information, see IP Domains (see page 36).

In a multi-tenant deployment, each tenant has its own groups. Tenant users cannot see items outside of the tenant group unless the global administrator grants such access with Service Provider groups.

Groups (Tenant)

Lets the global administrator or tenant administrator create custom groups. Select this node to enable the Add Group button.

Inventory (Tenant)

Includes all managed items that are associated with the tenant IP domains. Items from all registered data sources can appear in this group.

Each tenant also has the following system subgroups in its Inventory group:

IP Domains

Represents the IP domains that are associated with this tenant. Any managed items that have been discovered are associated with this tenant through its IP domains. To see the managed items of the tenant, click a tenant IP domain in the Groups tree.

Service Provider Defined Groups 

Includes groups that the global administrator has populated with shared items whose data this tenant can access. Use these groups to grant access to data from shared devices to selected tenant user accounts.

For example, a router that the service provider owns handles traffic from multiple tenant domains. Using Service Provider Defined groups, the global administrator can allocate tenant access to data from that router. This strategy lets the tenant perform some independent monitoring and verification of system performance.

Service Provider Items 

Contains all items that are not explicitly associated with a tenant IP domain. Such items are automatically placed in this group. The global administrator can then place these items into 'Service Provider Defined Groups' to allocate tenant access to data from shared items.

Permission Groups and Context Groups

"Permission groups" and "context groups" are terms that are applied to the same entities: custom groups. Permission groups are created to organize managed items for purposes of data access allocation. They are assigned to user accounts as permission sets. When permission groups are applied as filters to determine the data context for views and dashboard pages, they are named *context groups*.

Applying custom groups as permissions enables:

- Users to view data specifically within their area of responsibility, such as a physical location
- Administrators to restrict the users who can view data for security reasons

Users can also use the section of the Groups tree below their permission groups to change the data context for summary or group dashboards.

The groups that are assigned to your user account determine the data that you see in dashboards. The group that serves as a filter for the current dashboard is the *group context* for that dashboard. When you first log in to CA Performance Center, the pages that you see reflect the context of your default permission group.

You can change the context of all views on a dashboard page by selecting another context group. For more information, see Change the Group Context.

Groups and Data Sources

The read-only system groups are specific to data sources. Most system groups are only created when a data source is registered. Only the matching system groups are synchronized between the data sources and CA Performance Center.

By contrast, custom groups are sent down to all data sources during synchronization. In data sources that support drilldown, group structure is replicated in their reporting interface. Where supported, you can drill down from group names into data from individual group members.

For selected data sources, some restrictions on grouping apply. For example, CA eHealth groups cannot be copied into custom groups or site groups. They can only be used as standalone groups as they are configured in CA eHealth.

Use Groups to Customize Dashboards

When users log in to CA Performance Center, the dashboards that they see contain data from the default group that each user has permission to view. You can set a default group for each user in the user account settings. For example, an operator with primary responsibility for Site A, and functions as a backup for Site B, can view data for both groups. However, the default group setting lets this operator see only the Site A information by default.

You can use the default group feature to create one custom dashboard to represent every site in your enterprise.

Follow these steps:

1. Create custom groups to represent each site or branch office in your enterprise. Use names that clearly represent these locations.
2. Create a custom dashboard.
3. To monitor your locations, add the views that all operators use on a daily basis .

   Note: Add this dashboard to a menu that all users can see. The user account role determines menu access.

4. To select a new default group, edit each user account by following these steps:
   a. Log in as a user with administrative privileges.
   b. Navigate to the Manage Users page (see page 120).
   c. Select the user account that you want to change, and click Edit.
   d. Advance the wizard to the Permission Groups dialog.
   e. Use the Default Group drop-down list to select the group whose data this user can see by default.
   f. Click Save.
5. To set a different default group for each user, repeat the previous steps.

   When different users view the same custom dashboard, they see different data. The data are based on their default group.

Group Management

The Groups feature is a powerful tool that lets administrators organize data and control who can view it. When a performance issue is reported, the permission groups that are assigned to user accounts let operators effectively analyze data in a logical flow. They can drill down from averaged managed item data from all managed items to information about a single item in the same time frame.

The groups that you create, and the structure that contains them are key requirements for optimizing CA Performance Center. We recommend consulting with a CA technical representative to develop a strategy for assigning permission groups that meets your requirements.

Start working with groups on the Manage Groups page. This page displays the Groups tree (see page 62) in the left pane. The tabbed options in the right pane give access to group Items, Properties, and Rules (see page 76). To populate and edit groups (see page 83), use the options on these tabs.

View Group Membership

View a sortable list of all items that have been added to a system group or custom group on the Manage Groups page. You can verify group rules, or you can verify that custom scripts have appropriately created and populated groups. You can view all items, or a filtered list of items, in a selected group.

Distinguish custom groups, site groups, and system groups in the Groups tree by their icons. For more information, see Types of Groups (see page 62).

Filters can help you select the types of items you want to see, such as all items added to the group manually. By default, the list on the Items tab only displays items added directly to the group. The items are added either manually or by application of a rule (Direct items).

Follow these steps:

1. Log in as a user with the Administrator role, or use an operator account with the 'My Custom Groups' feature enabled.
2. Select Admin, Custom Settings, and click Groups. You can also click My Settings, My Custom Groups.

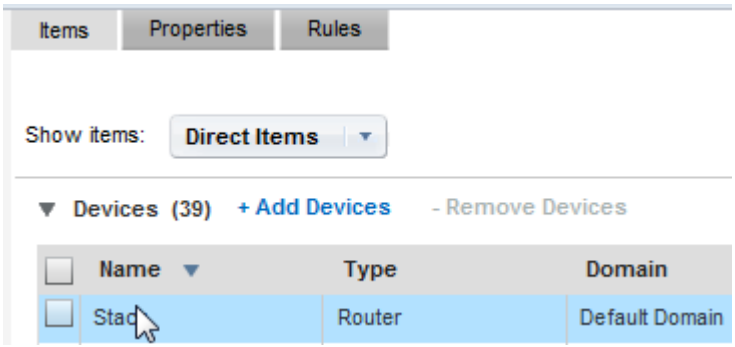
   The group management page appears.

   Note: Tenant administrators only see the items that are associated with their tenant.
3. To find the group whose membership you want to view, expand the nodes in the Groups tree in the left pane.

   Note: Groups that contain subgroups do not show any members on the Items tab. Expand these groups, and select a subgroup to view its members.
4. Select a group.

   The Items tab is selected in the right pane.

   Note: Custom groups also display a Rules tab.



   No items are shown by default.
5. Select a filter from the 'Show items' list to specify the items to display.
6. Click the arrow next to the item type name in the Show Items list. The following membership types are applicable, depending on the type of group that you selected:

   Direct Items

   Includes the items that were added directly to the group, either manually or by the application of a rule. You can add and remove items only when 'Direct Items' is selected. The 'Added By' column indicates whether the item was added manually (User) or by a group rule (Rule).

Direct and Inherited Items

Includes all items in the group, whether they were added directly or inherited as the children of items that were added directly.

A setting on the Properties tab determines the ability to inherit items. Excluded items are not inherited.

Inherited Items

Includes only the children of managed items in the group. When you enable inheritance for this group and add a router, all interfaces that are associated with the router are added to the group.

Inherited items cannot be removed individually. They are automatically removed when the parent item is removed.

Excluded

Refers to items that were added to the group because of a rule but later excluded by a group rule. Select this setting to see these items.

7. Select an item type from the list.

   A list of all items of the selected type that are included in the group appears. If necessary, click a link to scroll through multiple pages of items.

More information:

Create a Custom Group (see page 73)
Creating and Managing Groups (see page 61)
Types of Groups (see page 62)
Group Management (see page 71)
Add Managed Items to a Group Using Rules (see page 76)

Create a Custom Group

Before you start creating groups, plan a strategy and a structure. Consider the types of access permissions that CA Performance Center operators require to perform their monitoring duties. If necessary, you can discuss your organizational and monitoring goals with a CA technical representative. If you plan to deploy business hours, see Create a Site Group (see page 75) for more information.

Create groups under the 'All Groups' node in the Groups tree, or within an existing custom or site group. You cannot add groups to system groups, which appear "locked" in the Groups tree.

A maximum of 2000 child groups can be added to any parent group.

Important! If you create a group for a CA Infrastructure Management Data Aggregator data source, we recommend limiting group membership to 10,000 items. This count includes the children of managed items. Observing this limit keeps reporting time to less than 10 seconds.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The page displays current groups in a tree structure.
3. To find a location for the new group, expand the nodes in the Groups tree.
4. Right-click the node, and select Add Group.

   The Add Group window opens.

   The New tab is selected by default.
5. Supply values for the following parameters:

   Group Name

   Specifies a name for the group. Do not use the following special characters in group names: /&\,%.

   Description

   (Optional) Helps you identify the group.
6. Confirm the setting for the following parameter:

   Include the children of managed items

   Adds the children of managed items automatically when the items are added to this group. If you disable this option and add a router to the group, the interfaces on that router are not included. Therefore, their data is not visible in drilldown views.

   Default: Selected.
7. Select Custom from the Group Type list.
8. Click Save.

   The new group appears in the Groups tree.

   The group contains no items until you add them. You have two options for adding items to a custom group:

   - Manually populate the group by adding items in the Manage Groups interface.
   - Create rules to manage group membership.

More information:

Custom Groups (see page 65)
Permission Groups and Context Groups (see page 69)
Add Managed Items to a Group Manually (see page 81)
Add Managed Items to a Group Using Rules (see page 76)

Create a Site Group

Site groups are custom groups that are based on physical locations, such as a city, region, office, or campus. They include Time Zone and Business Hours parameters to let you precisely filter data from business-critical times of day.

Create site groups under the All Groups node in the Groups tree, or within an existing custom or site group. You cannot add a group to a system group, whose read-only status is indicated by a lock icon.

Site groups can contain subgroups. Create a hierarchical structure that helpfully reflects the geography and architecture of your IT infrastructure.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The page current groups appear in a tree structure.
3. Expand the nodes in the Groups tree to find the location where you want to create the new group.
4. Right-click, and select Add New Group.

   The Add Group window appears.
5. Supply values for the following parameters:

   Group Name

   Specifies a name for the group. Do not use the following special characters in group names: /&\,%.

   Description

   (Optional) Helps you identify the group.
6. Select Site from the Group Type list.

   The Location and Time Zone fields appear.

7. Enter the name of the geographical location that this site group represents.

   Use a physical location so that you can coordinate the managed items in this group with their appropriate time zone.

   Note: This name appears in data views to describe the site group.

8. Select a time zone for this site group from the list.

   Note: Time zones that are offset from UTC by a half-hour and a quarter-hour are not supported. Select the nearest full-hour time zone.

   The Business Hours parameter is enabled.

9. Select a custom business-hours definition from the list. Business-hours definitions are created in a separate procedure.

10. Click Save.

    The new site group appears in the Groups tree.

11. Continue creating the site groups that are required to represent all of the distinct sites or time zones in your enterprise.

    A site group contains no items until you add them. You have two options for adding items to a custom group:

    - Manually populate the group by adding items in the Manage Groups interface (see page 81).
    - Create rules to manage group membership (see page 76).

More information:

Create a Custom Group (see page 73)
Types of Groups (see page 62)
Create Business-Hour Definitions (see page 57)

Add Managed Items to a Group Using Rules

Networks and systems are constantly changing. CA Performance Center system groups are automatically updated to include managed items as they are discovered. However, it can be difficult to keep custom groups up-to-date. Therefore, you can use rules to populate the custom groups in your monitoring system. Newly discovered items that meet rule specifications are added to groups. Similarly, items that do not meet rule requirements, or items that are no longer monitored, are removed.

Important! If you create a group for a CA Infrastructure Management Data Aggregator data source, we recommend limiting group membership to 10,000 items. This count includes the children of managed items. Observing this limit keeps reporting time to less than 10 seconds.

Before you create rules, take some time to define the items that you want to add to your grouping structure. Group rules are best implemented as part of an overall grouping strategy to organize managed items and provide operator access to associated data. You can still add items manually to groups with existing rules.

Note: Group rules do not apply to domain groups.

Follow these steps:

1. Navigate to the Manage Groups page (see page 71).

   The page displays current groups in a tree structure.

2. Select the group that you want to populate in the Groups tree.

   If items have already been added to this group, they appear in the right pane.

   Note: Items that are added directly to a group as a manual step appear as Direct Items in the Group Properties pane. Items that are added to a group because they are children of a managed item are Inherited Items in the Group Properties.

3. Click the Properties tab in the right pane.

   The Properties page opens.

4. Confirm the setting for the following option, and change it if necessary:

   Include the children of managed items

   Adds the children of managed items automatically when the items are added to this group. If you disable this option and add a router to the group, the interfaces on that router are not included. Therefore, their data is not visible in drilldown views.

   Default: Selected.

5. Click Save.

6. Click the Rules tab, and then click Add Rule.

   The Add Rule dialog opens.

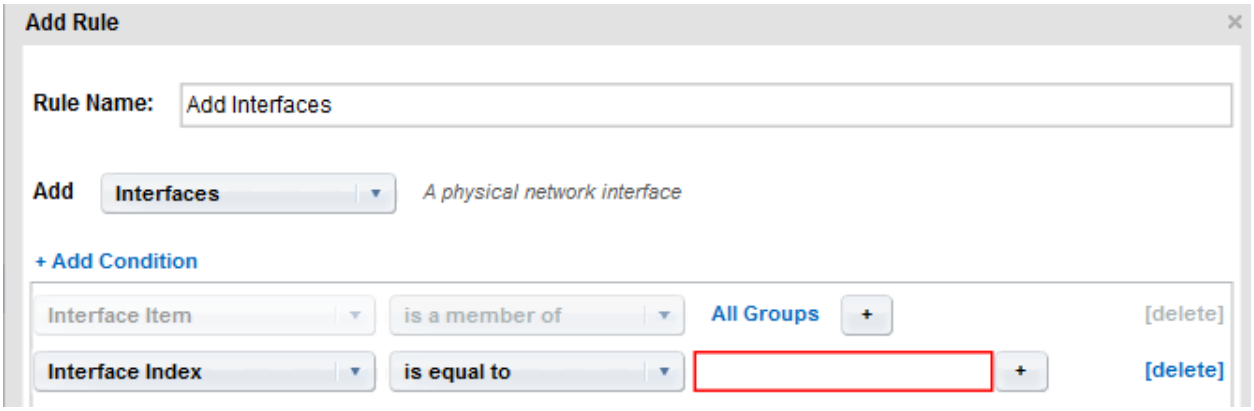
7. Supply a name for the rule in the Rule Name field.

8. Select the type of managed item that you would like to add to the group from the Add list.

   Available options vary based on the data sources that are registered with CA Performance Center.

9. Click Add Condition.

   A row of drop-down lists and fields appears.



10. In the first list, select a method for identifying managed items. For example, select Device Type. The options include item description, name, type, location, contact person, model, vendor, object ID, and IP address. The "Name" and "Name Alias" items are available to users, depending on the role rights that the administrator sets.

    The remaining lists are updated to match the type of item selected.

    Note: The methods for identifying managed items vary based on the managed item selected.

11. Select a method for matching from the second list. For example, select 'is equal to'.

    Important! When adding a network subnet condition, use CIDR notation for the IP addresses that you supply for the 'is in subnet' and 'is not in subnet' options. Use dotted-decimal notation for the IP addresses that you supply for the 'is between' and 'is not between' options.

12. (Optional) Enter text to match in the remaining condition field. For example, to add all routers and servers in the Southwest region, enter text that corresponds to the appropriate naming convention, such as "sw*".

    Note: Wildcard characters are accepted in this field, such as an asterisk (*) for a multicharacter match.

13. (Optional) To add 'OR' matches, click + at the end of the condition.

    An 'OR' field appears.

14. (Optional) To add 'AND' matches, click Add Condition. By default, every new condition that is added is connected to every other condition with an AND statement.

    Three more drop-down lists appear.

    Note: An 'AND' condition indicator does not appear. By contrast, an 'OR' indicator appears when you select an 'OR' operator.

15. Click Preview Results to confirm that the new rule is including the items that you want.

    The results are shown in the Group Rules Preview window. You can expand each item type to see the specific items added.

16. (Optional) Click +Add Rule to add other item types to the group.

    Each item type requires its own rule.

17. When you have finished creating rules, you can click Save or Save and Run Rules:

    - Save - Saves the rules without running the rules. The group is populated during the next global synchronization, which occurs approximately every 5 minutes.
    - Save and Run Rules - Saves the rules and populates the group immediately.

Edit a Group Rule

Group rules automatically add managed items to custom groups as items are discovered during monitoring. Once you have created a rule, you can edit it. When you edit a rule, you can modify or delete filters, or add subrules.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The current groups appear in a tree structure.
3. Expand the All Groups node in the Groups tree.
4. Select the group with the rule that you want to modify.
5. Click the Rules tab.
6. Use the mouse to hover over the rule.

   Options to edit or delete the rule appear.
7. Click Edit.

   The Edit Rule window appears.
8. Make the desired changes to existing filters, add filters or subrules, or remove filters or subrules as needed.
9. Click OK.
10. Click Preview Results to confirm that the modified rule adds the appropriate items the group. If necessary, edit the rule again.

11. When you have finished editing the rules, click one of the following options:

    Save

    Saves the rules without running them. The group is populated during the next global synchronization. Global synchronization occurs approximately every 5 minutes.

    Save and Run Rules

    Saves the rules and populates the group immediately.

Add a Subrule to a Group Rule

You can add a subrule to any group rule that you have created. Group rules add managed items automatically to a custom group as items are discovered during monitoring. Subrules extend the rule intelligence to other items, or more narrowly define the filters in the original rule.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The current groups appear in a tree structure.
3. Select the group containing the rule that you want to modify.
4. Click the Rules tab.
5. Click the rule to expand it.

   The rule definition text and the Add Subrule link appear.
6. Click Add Subrule.

   The Add Rule window appears.

   The options are identical to the options that applied to the original rule.
7. Select the desired options by selecting the Type of the items to add from the dropdown, and setting up filters as needed.
8. Click OK.
9. Click Preview Results to confirm that the modified rule adds the appropriate items to the group.

   If necessary, edit the rule again.
10. When you have finished editing rules, click one of the following options:
    - Save - Saves the rules without running them. The group is populated during the next global synchronization. Global synchronization occurs approximately every 5 minutes.
    - Save and Run Rules - Saves the rules and populates the group immediately.

Delete a Group Rule

You can delete the rules that you have created to add managed items to a group automatically. Deleting a group rule immediately removes any items added to the group to which the rule was applied. The items are not deleted from the inventory, but they are no longer available on the Items tab for the affected group.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The page displays the current groups in a tree structure.
3. Select the group with the rule that you want to delete in the Groups tree.
4. Click the Rules tab.
5. Hover the mouse cursor over the rule.

   The Edit and Delete options appear as links.
6. Click Delete.

   A confirmation dialog appears.
7. Click Delete.

   The rule is no longer applied to the group. Any managed items that match the group rule are removed from the group.

Add Managed Items to a Group Manually

You can populate custom groups manually, by adding managed items. Individually adding managed items to groups can be necessary when you are fine-tuning group structure. However, setting up group rules is usually a more effective strategy.

Important! If you create a group for a CA Infrastructure Management Data Aggregator data source, we recommend limiting group membership to 10,000 items. This count includes the children of managed items. Observing this limit keeps reporting time to less than 10 seconds.

Follow these steps:

1. Navigate to the Manage Groups page (see page 71).

   The current groups appear in a tree structure.

   Note: System groups appear with a "lock" symbol in the Groups tree to indicate their read-only status. You cannot add items to or remove them from system groups.

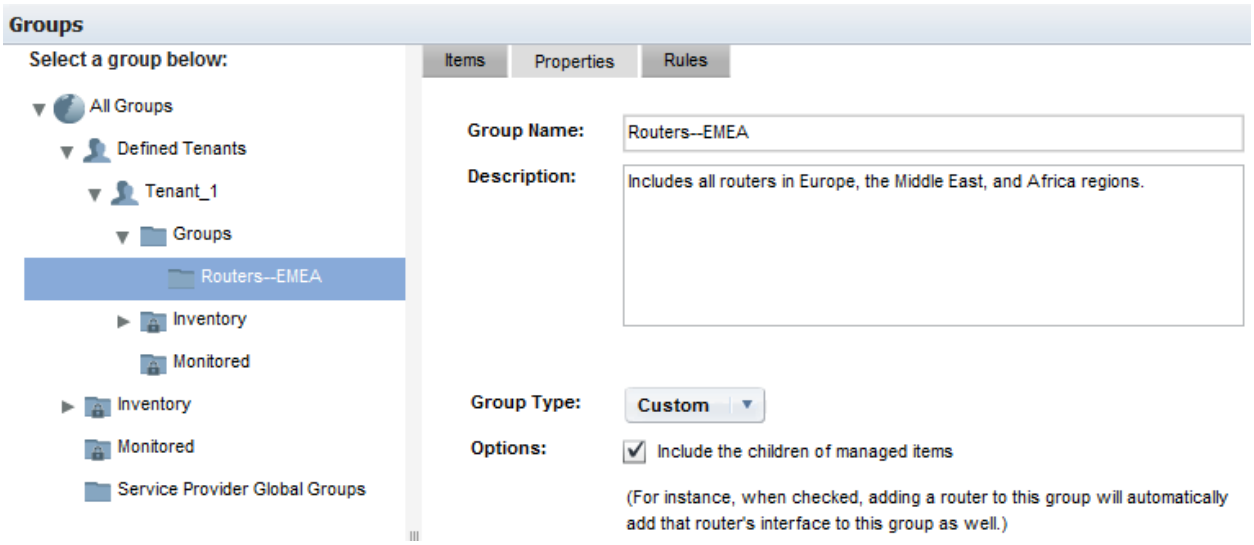
2. Expand the nodes in the Groups tree to locate and select the group to which you want to add managed items.

   Items that have already been added to this group appear in the right pane.

   Note: Items that are added directly to a group as a manual step appear as Direct Items in the Group Properties pane. Items that are added to a group because they are children of a managed item are Inherited Items in the Group Properties.

3. Click the Properties tab in the right pane.

   The Properties page opens.



4. Confirm the setting for the following option, and change it if necessary:

   Include the children of managed items

   Adds the children of managed items automatically when the items are added to this group. If you disable this option and add a router to the group, the interfaces on that router are not included. Therefore, their data is not visible in drilldown views.

   Default: Selected.

5. Click Save.

6. Click the Items tab.

   The Show Items list appears. The Show Items list only applies to groups that contain members.

7. Click Add Item Type.

   The Add Items dialog opens.

8. Select the type of item that you want to add from the Available Items list.

   The list of items refreshes to show items of the selected type that are available to add to the group.

   The available items depend on the item type, the data sources that are registered, and the items that are discovered.

9. To see more pages of items, click the links below the list.

   You can also use the Search field to search for an item in the list.

10. To select one or more items, click the check boxes next to the items.

    To select all items on a page, click the check box in the table header row.

11. Click Add Items.

    The Items tab refreshes to show the new group members, but the Add Items dialog remains open.

12. Click Close when you have finished adding items.

    The Add Items dialog closes.

    The Items tab shows the items that you have added.

Copy a Subgroup into a Group

After you have created custom groups, you can populate groups by adding subgroups that contain managed items. You can add new groups to existing groups. The new groups become subgroups in a hierarchical structure. You can also copy system groups or other custom groups into high-level groups to create subgroups.

When you copy a group, you are actually creating a *group reference*. You cannot modify a group reference, but you can remove it. Groups that have been copied display an extra tab in the right pane. Click the Remove References tab to see places where copies of this group have been placed.

Any changes that you make to the original group are reflected in all of the references of the group. Removing a group also deletes all of its references.

Important! If you create a group for a CA Infrastructure Management Data Aggregator data source, we recommend limiting group membership to 10,000 items. This count includes the children of managed items. Observing this limit keeps reporting time to less than 10 seconds.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The page displays current groups in a tree structure.

3. Expand nodes in the Groups tree to locate and select the group that you want to copy. All of its subgroups are automatically included in the selection.
4. Right-click, and select Copy Group.
5. Select the parent group where you want to add the subgroup.
6. Right-click, and select Paste Group.

   The existing group and all of its subgroups are copied to the selected parent group.

   Their icons now indicate that they are read-only group references  .

Add Subgroups to a Group

To create a hierarchical structure, you can create new groups within custom groups that you created previously. You can also add an existing group to another group so that it becomes a subgroup.

Important! If you create a group for a CA Infrastructure Management Data Aggregator data source, we recommend limiting group membership to 10,000 items. This count includes the children of managed items. Observing this limit keeps reporting time to less than 10 seconds.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The current groups appear in a tree structure.
3. Expand nodes in the Groups tree to locate and select the parent group.
4. Right-click, and select Add New Group.

   The Add Group dialog appears.
5. Select the Existing tab.

   The Groups tree appears.
6. Navigate to the group that you want to add as a subgroup, and select it.

   Any subgroups of the selected group are automatically included in the selection.
7. Click Select.

   The existing group and all of its subgroups are added to the selected parent group.

(new related group 1)

Delete a Group Reference (see page 85)

Delete a Group

The CA Performance Center global administrator can delete custom groups, including groups that belong to any tenants. A tenant administrator can also delete custom groups that belong to that tenant definition. The subgroups of the deleted group are also deleted.

Note: System groups cannot be deleted. Likewise, the Default Domain group cannot be deleted.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Groups page (see page 71).

   The page displays current groups in a tree structure.
3. Select the group that you want to delete from the Groups tree. To delete a group that contains subgroups, select the highest level of the groups that you want to remove.
4. Right-click a group, and select Remove Group.

   A confirmation dialog appears.
5. Click Yes to confirm the deletion.

   The selected group and all of its subgroups are deleted.

Note: Follow a slightly different procedure to Delete a Group Reference (see page 85). A group reference is a copy of another group. Its icon indicates that it is a copy: 

Delete a Group Reference

A group reference is a copy of another group. Its icon indicates that it is a copy:  You can delete group references by using the References tab for the original group. All groups that have been referenced somewhere in the Groups tree have an extra tab in the right pane. Use the "Remove References" tab to see and remove references to that group.

Deleting a group that has been referenced deletes all of its references. By contrast, if you delete a group reference, the original group is not affected.

Deleting a subgroup that is a reference does not affect the original group or the group that contains it. To delete a group that contains subgroup references, delete all of the references before deleting the group. Otherwise, issues arise when you attempt to remove the references.

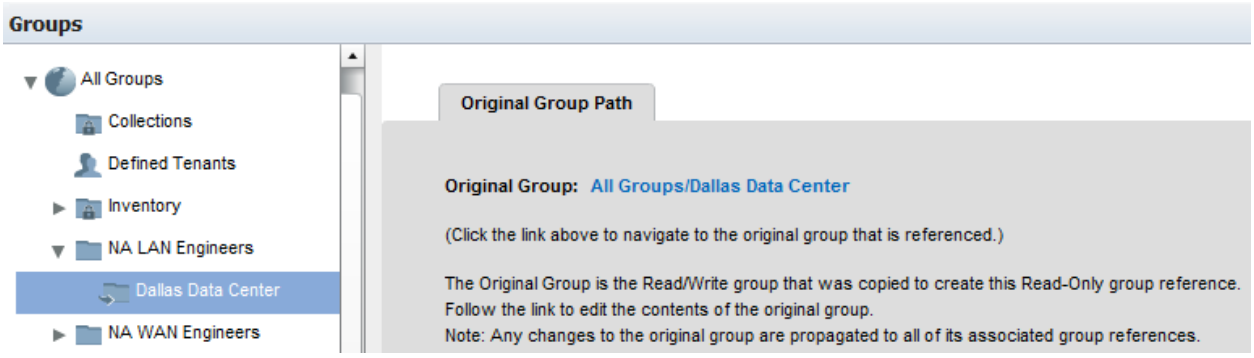
For example, if several offices consolidate in a single location, delete all references to the closed offices to prevent them from appearing in search results. Deleting one reference does not delete them all.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Groups page (see page 71).

   The current groups appear in a tree structure.
3. Find the group reference that you want to delete.
4. Select the group reference.

   In the right pane, a link to the original group that was copied appears.



5. Click the Original Group link to navigate to the original group.

   The original group appears, with a new tab in the right pane.
6. Select the Remove References tab.

   All references to this group are listed. The path of the references is included in the Groups tree.
7. Select the group reference that you want to delete.
8. Click Remove Group Reference.

   A confirmation dialog appears.

9. Click OK to confirm the deletion.

   The selected group reference is deleted.

Chapter 4: Creating and Managing Roles

This section contains the following topics:

Roles

The *role* is a parameter assigned to a user account that controls user access to product features and dashboard pages. Based on user job functions, the role grants administrative access to product configuration using *role rights*. Roles let users access data and product features that they require to perform their duties and restrict access to features that they do not require.

CA Performance Center shares roles with registered data sources. User roles determine what users can see and do in the data source interface when following a drilldown path to a data source.

When you add a user to CA Performance Center, you select a role for the user account. You The *role* is a parameter assigned to a user account that controls user access to product features and dashboard pages. Based on user job functions, the role grants administrative access to product configuration using *role rights*. Roles let users access data and product features that they require to perform their duties and restrict access to features that they do not require. existing roles to meet the unique needs of users in their environment.

You can edit roles to include new role rights. And you can disable roles to prevent users with those role assignments from using CA Performance Center.

A set of predefined, or "factory," roles help you to add new users quickly while determining what customizations are needed.

Predefined Roles

The following table describes the roles that are included with CA Performance Center by default ("factory" roles):

Name of Role	Menus	Rights
Administrator	All	All rights, including the unique role right to Administer Data Sources. Also includes access to features with no corresponding role right. For example, only users with this role can create tenants, IP domains, SNMP profiles, and shared custom groups. **Note**: This role is the global administrator. Only the role right to view SNMP security data in clear text can be modified.
Tenant Administrator	All	This role only supports the Data Aggregator data source. All rights, including the unique Administer Tenants role right. Does *not* include access to groups that are part of the Default Tenant workspace. Does *not* have access to the default domain.

Name of Role	Menus	Rights
Designer	All	■ Administer Menus ■ Administer Roles ■ Administer Shared Dashboards ■ Create a Dashboard ■ Drill into Views ■ Edit Context Pages ■ Edit Shared Views ■ Edit Time Zone ■ Export to CSV ■ Generate URLs from Views ■ Print a Dashboard ■ Proxy Users ■ Save Changes to Shared Views ■ Send Reports by Email ■ Send Reports on a Schedule ■ View Conversations ■ View Hosts ■ View Inventory and Search ■ View Protocols ■ View ToS

Name of Role	Menus	Rights
IT Architect	All	■ Administer Shared Dashboards ■ Create a Dashboard ■ Create Notifications ■ Drill into Data Sources ■ Drill into Views ■ Edit Shared Views ■ Edit Time Zone ■ Export to CSV ■ Generate URLs from Views ■ Print a Dashboard ■ Save Changes to Shared Views ■ Send Reports by Email ■ Send Reports on a Schedule ■ All rights to view data. See the Designer role for the full list.
IT Director	All	■ Administer Shared Dashboards ■ Create a Dashboard ■ Drill into Views ■ Edit Time Zone ■ Export to CSV ■ Generate URLs from Views ■ Print a Dashboard ■ Send Reports by Email ■ Send Reports on a Schedule ■ All rights to view data. See the Designer role for the full list.

Name of Role	Menus	Rights
IT Engineer	My Dashboards Engineering Operations Displays Applications	■ Administer Shared Dashboards ■ Create a Dashboard ■ Drill into Views ■ Edit Shared Views ■ Edit Time Zone ■ Generate URLs from Views ■ Print a Dashboard ■ Save Changes to Shared Views ■ Send Reports by Email ■ All rights to view data. See the Designer role for the full list.
IT Manager	My Dashboards Operations Displays Capacity Planning Management Applications	■ Administer Shared Dashboards ■ Create a Dashboard ■ Create Notifications ■ Drill into Views ■ Edit Shared Views ■ Edit Time Zone ■ Generate URLs from Views ■ Print a Dashboard ■ Save Changes to Shared Views ■ Send Reports by Email ■ Send Reports on a Schedule ■ All rights to view data. See the Designer role for the full list.
IT Operator	Infrastructure Health Operations Displays	■ Create Notifications ■ Drill in to Views ■ Edit Time Zone ■ Print a Dashboard ■ Send Reports by Email ■ All rights to view data. See the Designer role for the full list.

Name of Role	Menus	Rights
Operations Center Manager	My Dashboards Operations Displays	■ Create a Dashboard ■ Create Notifications ■ Drill into Views ■ Edit Shared Views ■ Edit Time Zone ■ Export to CSV ■ Generate URLs from Views ■ Print a Dashboard ■ Proxy Users ■ Save Changes to Shared Views ■ Send Reports by Email ■ Send Reports on a Schedule ■ All rights to view data. See the Designer role for the full list.
VP of IT	My Dashboards Capacity Planning Management	■ Create a Dashboard ■ Drill into Views ■ Edit Shared Views ■ Edit Time Zone ■ Export to CSV ■ Print a Dashboard ■ Save Changes to Shared Views ■ Send Reports by Email ■ All rights to view data. See the Designer role for the full list.

Note: The predefined administrator account, 'admin', has the Administrator role. The predefined user account, 'user', has the IT Operator role. You can modify the two predefined user accounts, admin and user, by changing the name and the password, for example. Only limited modifications are enabled for the ‘Administrator’ role. We recommend changing the default passwords for better security.

More information:

Role Rights (see page 95)
View Current Roles (see page 103)

Role Rights

The rights assigned to each role determine user access to dashboards and menus. Role rights determine the types of views that users can see and whether they can export data and customize settings.

Administrators can grant additional rights to users by editing their role. The Edit Role dialog lists role rights currently assigned to roles. And the Manage Users page shows the role assigned to each user.

Note: Do not remove the administrative role rights from your primary administrator account. Administrative access to the console is required.

The following list describes the available access rights to CA Performance Center features:

Administrative Role Rights

The following role rights give users access to administrative features. Limit the number of users with these role rights for increased security.

Create DA Threshold Profiles

Lets users define and configure threshold profiles. Each user can only edit the profiles that he or she created. Unlike the Administer DA Threshold Profiles role right, this role right does not allow users to configure profiles that were created by other users, or to transfer ownership of profiles.

Administer Data Sources

Lets users register new data sources, test data source connections, view data source status, change data source parameters, and remove data sources. Also lets users view the data source log.

Administer Groups

Lets users without full administrative rights manage a specific branch of the Groups tree. With this role right, users can create, change, and delete groups only in the specified branch. The Administrator role and the Tenant Administrator role have this role right by default, allowing administration of All Groups and the Tenant root group, respectively.

Only the Administrator and the owner (creator) of the groups in the administered branch can delete groups in that branch. When an administered group is a child of another group (that is, a subgroup), the administered group is deleted when the parent group is deleted. Administered groups are not deleted when the user account of the owner is deleted.

Notes:

- Assign this role right to users who should not have *full* administrator rights to the Groups tree, but instead require limited, branch-specific administrator rights. In some organizations, this user might be a 'power user' or a 'super user.'
- Do not confuse the 'Administer Groups' role right with the 'My Custom Groups' feature, which is simply a tool that lets users organize the groups to which an administrator has granted them access. 'My Custom Groups' does not provide administrative rights to a specific branch of the Groups tree.

Administer Menus

Lets users create, edit, and delete menus. This role right is required to assign new dashboards to menus. To assign menus to user accounts, the 'Administer Roles' role right is required.

Administer Roles

Lets users create, edit, and delete user account roles. Lets users assign new menus to user accounts by editing roles.

Administer Shared Dashboards

Lets users manage their own and other users' dashboards. They can edit an existing dashboard page and save changes that are visible to other users.

- To create a dashboard, the 'Create a Dashboard' role right is required.
- To assign a dashboard to a menu, the 'Administer Menus' role right is required.

Administer Tenants

Grants users administrative rights over the tenants that are selected in the user wizard. Users with this role have the rights to administer certain tenants while having limited access to the default tenant. This role is only used in multi-tenant environments. Tenant administration includes the ability to manage:

- Users
- Menus
- Dashboards
- Views

Administer Users

Lets users create, edit, and delete user accounts. Lets users assign new roles to user accounts.

Create DA Threshold Profiles

Lets users define and configure threshold profiles. Each user can only edit the profiles that he or she created. Unlike the Administer DA Threshold Profiles role right, this role right does not allow users to configure profiles that were created by other users, or to transfer ownership of profiles.

Create a Dashboard

Lets users create new dashboards and populate them with views. Other users cannot see these dashboards. To create dashboards for other users, the 'Administer Shared Dashboards' role right is required.

Create Notifications

Lets users configure email notifications using the Create/Edit Notifications wizard from the Admin, Notification menu. Notifications are not supported for all data sources. The CA Performance Center Readme file contains an up-to-date list.

Create On-Demand Report Templates

Lets users create, edit, and delete on-demand report templates. This role right is always assigned together with the Run On-Demand Report Templates right. Users can save on-demand report templates at the user level, which allows only the user to view the templates. Users can also save on-demand report templates at the tenant level, which allows all users within the tenant to view the template.

Delete Data Sources

Lets a user with the Administrator role delete (unregister) a data source. Not assigned to any user or role by default. Can only be assigned to the Administrator role.

Drill from Views into DA Admin Page

Lets a user access the Data Aggregator administrator page directly from a page that is associated with the Data Aggregator. For this role right to work properly, the user must also have the Administer Data Sources right. The ability to access the Data Aggregator administrator page is limited to views for Data Aggregator devices, interfaces, and components. Selecting a Data Aggregator interface or component causes the administrator page for the associated parent device to appear when clicking the gear  button and Device Admin.

Edit Context Pages

Lets users edit, delete, add, or reorder tabs on context pages. A *context* is a managed item, such as a device, a router, a switch, or an interface. A context page resembles a dashboard with a fixed context. Only the Designer and Administrator roles have this right by default.

Proxy Users

Lets users log in as a selected user to view and verify user account settings.

Save Changes to Shared Views

Lets users save edits they have made to the views on a shared page. Other users who can see these views can see the changes if they are applied as a 'Default for All Users'. The changes can also be saved to the user account so that they persist after logout.

SNMP Clear Text

Lets users troubleshoot SNMP profiles and view security information that is typically masked in clear text.

Role Rights for Dashboard and View Access

The following role rights give users access to reporting features. Most user accounts require these rights.

Drill into Data Sources

Lets users navigate to the data source interface during drilldown to see detailed data from a selected item.

Drill into Views

Lets users drill in to a CA Performance Center context view to see detailed data from a selected item. Required to enable the 'Edit Context Pages' role right.

Edit Shared Views

Lets users edit the views on a shared page for themselves. Other users who can see these views cannot see the changes. The changes can only be applied to the current login session or saved to the current user account.

Edit Time Zone

Lets users edit their own time zone setting for data displayed in dashboards.

View Conversations

Lets users see specific client conversations.

View Hosts

Lets users see specific client host information.

View Item Display Name or Name Alias

Lets users see the display names or the aliases for items.

Note: Users who are given this role right can select which name to display in their dashboards and views in the My Settings, Display Settings menu item.

View Item Name Alias Only

Lets users see only the aliases for items.

View Inventory and Search

Determines whether users can access the Inventory tab and Search field to find items.

View Protocols

Lets users see protocol information where available.

View ToS

Lets users see the Type of Service information in applicable views.

Role Rights to Export and Print

The following role rights give users the ability to export dashboard data in various formats:

Export to CSV

Lets users export the contents of a selected view to a file in comma-separated values (CSV) format.

Generate URLs for views

Lets users share views externally with a URL.

Print a Dashboard

Lets users export the current dashboard page as a PDF and send it to a selected printer.

Send Reports by Email

Lets users export dashboards as reports and send them to other users in email messages from the console.

Send Reports on a Schedule

Lets users set up schedules to export dashboards as reports and automatically send them by email on a recurring basis.

Note: This right also requires the 'Send Reports by Email' role right.

Run On-Demand Report Templates

Lets users run on-demand report templates. This role right is always given together with the Create On-Demand Report Templates right. However, if the Create On-Demand Report Templates right is taken away, users do not lose the ability to edit and delete their on-demand dashboards. Users who have this right without the Create On-Demand Templates right can run on-demand report templates on the tenant level.

Run Dashboards at Higher Resolution

Lets users select higher resolutions when viewing dashboards. No roles in CA Performance Center are given this role right by default. Users with this role right can set and save the resolution to higher values than are typically allowed when reporting for longer time ranges. When users save the higher resolution at the tenant level, it is only visible to users with this role right.

Note: When a higher resolution is set, some charts may still display other resolutions for NULL data.

Role rights also include menus. You can grant access to selected custom and predefined menus by editing role rights.

More information:

Add a Role (see page 104)
Data Source-Specific Role Rights (see page 100)
Predefined Roles (see page 90)

Data Source-Specific Role Rights

Each data source that is registered with CA Performance Center has its own set of roles with unique rights to features and data within that interface. Administrators can assign rights for a role within that data source through CA Performance Center. These data source rights apply when users follow a drilldown path from a CA Performance Center data view to that particular data source. However, any rights that are granted in this manner are specific to a data source instance. For example, if more than one CA Application Delivery Analysis data source is registered, the rights for each management console are managed separately.

For example, an administrator can grant the right to generate reports in a CA Network Flow Analysis data source, but withhold the right to edit dashboards in CA Performance Center. The individual data source *Administrator Guides* provide detailed information about how role rights are applied.

Individual data source administrators can create user accounts and grant users role rights to access features within that data source. After registration, those rights are synchronized with CA Performance Center and displayed on the Edit Role page.

Note: Role rights to individual data sources are distinct from rights to access CA Performance Center features; however, they frequently have the same names.

The following topics summarize the rights available to users of each data source.

Data Aggregator Role Rights

Name of Role Right	Description
Drill from Views into DA Admin Page	Drill down from Data Aggregator views to the Monitored Devices Admin page to troubleshoot a view that does not display data.
Administer Tenants	Administer tenants, including user accounts, discover and delete devices for Data Aggregator.
Administer DA Threshold Profiles	Administer Data Aggregator threshold profiles, including creating threshold profiles, editing any threshold profiles, and changing the ownership of all threshold profiles.
Create DA Threshold Profiles	Create Data Aggregator threshold profiles, where you can create and manage event profiles. Event profiles contain event rules, and are associated with groups. You can create reports on the events that are generated with these profiles. This role allows you to create threshold profiles, edit your own profiles, and view all threshold profiles.

CA Network Flow Analysis Role Rights

The following table summarizes role rights applicable to the CA Network Flow Analysis (formerly CA ReporterAnalyzer) console:

Name of Role Right	Description
View ToS	View Type of Service data
Manage Reports	Create, modify, delete, and execute reports
Run Reports	Execute defined reports
View Conversations	View conversation data
View Hosts	View host data
View Protocols	View protocol data

CA Application Delivery Analysis Role Rights

The following table summarizes role rights applicable to the CA Application Delivery Analysis (formerly NetQoS SuperAgent) management console:

Name of Role Right	Description
Engineering	Navigate the Engineering section; create Engineering reports
Operations	Navigate to the Operations section; create Operations reports
Management	Navigate the Management section; create Management reports
Incidents	Navigate the Incidents section; view Incidents reports
Investigations	Launch Investigations; drill into data from Investigations

Role rights do not give a CA Application Delivery Analysis user:

- Permission to access the Administration page of the CA Application Delivery Analysis management console.

  To give a user access to the Administration page, give the user the Administrator or Power User product privilege on the CA Application Delivery Analysis data source.

- Access to actual report data in the CA Application Delivery Analysis management console.

  To enable a user to see report data, assign the appropriate groups to the user.

CA Unified Communications Monitor Role Rights

The following table summarizes role rights applicable to the CA Unified Communications Monitor management console:

Role Right	Description
Call Details	Export call details to a CSV file
Call Performance	Access Call Performance reports
Call Quality and Volume	Access Call Quality and Volume reports
Call Watch	Access Call Watch reports
Call Watch Setup	Set up and launch a Call Watch on a selected phone
Collector Incidents	Access Collector Incident reports

Role Right	Description
Incidents	Access Incident reports
Investigations	Access Investigation reports
Launch Investigation	Launch an investigation and view the resulting data
Phone Details	Access Phone Details reports
Quality	Access Quality reports
Trunk Groups	Access Trunk Group reports
Voice Interface	Access Voice Interface reports
Midstream Devices	Access midstream device and midstream legs reports

View Current Roles

CA Performance Center includes a set of predefined ("factory") roles that you can assign to custom user accounts. You can access summary information about these roles on the Manage Roles page. Any custom roles that you create are also listed on this page.

Follow these steps:

1. Log in as a user with administrative role rights (see page 95).
2. Select Admin, User Settings, and click Roles.

   The Manage Roles page shows a list of currently defined roles that are available for assignment to user accounts.

   Note: Tenant administrators only see the items that are associated with their tenant.

   The table includes the following information about each role:

   Role Name

   Is the name of the role. The names of factory roles are based on common Information Technology job categories.

   Description

   Describes the job function of the person who is typically associated with a particular role.

Status

Shows the status of this role, either Enabled or Disabled. A role can be disabled for security purposes.

Users

Shows the number of user accounts that currently have this role assignment.

To perform any action on this page, select a role, and then click a button. Edit a role to see the list of menus and role rights that are assigned to it.

More information:

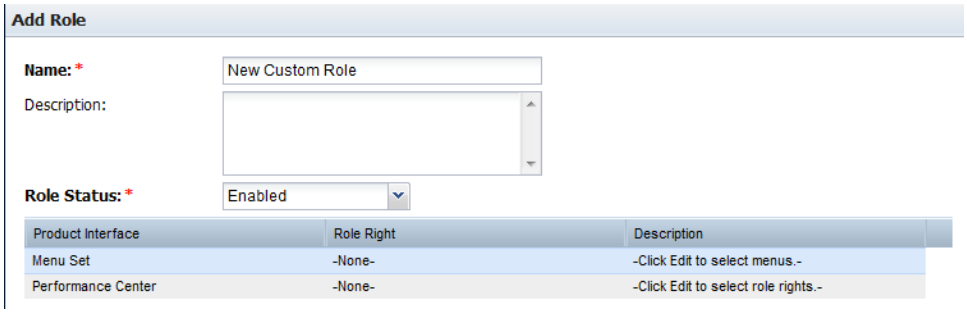
Add a Role (see page 104)
Predefined Roles (see page 90)
Edit a Role (see page 106)

Add a Role

If the predefined user roles (see page 90) provided with CA Performance Center do not fit your requirements, you can add custom user roles. Ideally, you create the roles that each unique product operator requires to perform job responsibilities.

Custom roles work best within a system of custom groups. Custom groups let you precisely grant access to dashboards and product features while restricting access to sensitive data. The same groups that you create to organize data can serve as "permission groups" when you set up user account permissions.

A new role has no role rights until you add them.



Note: When you have finished creating a role, assign it to a user account as a separate step. Roles are inoperative until they are assigned to user accounts. Only users with the 'Administer Users' and 'Administer Roles' role rights can assign roles to user accounts.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).

2. Navigate to the Manage Roles page (see page 103).

   The current list of roles appears.

3. Click New.

   The Add Role dialog opens.

4. Supply the required information and make selections in the fields provided:

   Name

   (Optional) Identifies the role. Limited to 45 characters.

   Description

   (Optional) Describes the role. For example, identifies the job-related duties that the associated user performs.

   Enable Role

   Enables the role to make it active. Required to give users with this role the access granted by role rights.

5. Select Menu Set, and click Edit.

   The Edit Menu Set dialog opens. Menus that are listed in the 'Available Menus' list can be added to the role.

6. Click an item on the left that you want to add to the role, and then click the right arrow.

   Use Shift + Click or Ctrl + Click to select multiple items in the list.

   The selected item moves to the Selected Menus list.

7. (Optional) Use the Up and Down arrows to move items around in the list. The order of menus in the list determines their order on the Dashboards tab.

8. Click Save.

   You return to the Add Role page.

9. Select Performance Center, and click Edit.

   The Edit Role Rights dialog opens, where you can select individual access rights for this role. Role rights that are listed in the 'Available Rights' list can be added to the role. For more information, see Role Rights (see page 95).

10. Click an item on the left that you want to add to the role. Then, click the right arrow to move it to the Selected Rights list.

11. (Optional) Use the Up and Down arrows to move items around in the list. The order of role rights determines their priority in cases where rights overlap.

12. Click Save.

    You return to the Add Role page.

13. Click Save.

    The new role is created and appears in the Role List.

More information:

Role Rights (see page 95)
Data Source-Specific Role Rights (see page 100)

Edit a Role

The predefined user roles (see page 90) are useful for getting operators started using CA Performance Center. You can modify predefined roles, or you can create new rules to suit your unique environment and the responsibilities of product operators.

Global administrators and users with the required role rights can modify both predefined and custom roles. Tenant administrators only have access to the roles associated with their tenant.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Roles page (see page 103).

   The page displays the current list of roles.
3. (Optional) Check the current usage of the role you want to modify, as follows:
   a. Select the role.
   b. Click Users to open the User List page, which is filtered to show only users who are assigned to the selected role.
   c. Click Roles to return to the Manage Roles page.
4. Select a role that you want to edit.
5. Click Edit.

   The Edit Role dialog opens.
6. Modify role settings (see page 104) as required.

   A table lists the role rights that have been selected for the role.
7. Select Performance Center, and click Edit.

   The Edit Role Rights dialog lets you select individual access rights for this role. For more information, see Role Rights (see page 95).

8. Select an item on the left that you want to add to the role. Click the right arrow to move it from the Available Rights list to the Selected Rights list.

   Use Shift + Click or Ctrl + Click to select multiple items in the list.

9. (Optional) To add a menu to this role:

   a. Select Menu Set, and click Edit.

   b. Select the new menu in the Available Rights list.

   c. Click the right arrow button to move it to the Selected Rights list.

   d. (Optional) Use the Up and Down arrows to change the order of menus in the list of selected menus.

   e. Click OK when you have finished adding menus.

   Note: You can assign a maximum of six menus to a role, including the My Dashboards menu.

10. Click Save.

    The changes to the role are saved.

More info

Add a Role (see page 104)
Role Rights (see page 95)

Delete a Role

You can delete any custom role that you have created. To delete a role, the role must not be assigned to any user accounts.

Note: The Administrator role cannot be deleted or disabled. You can delete any other role that lacks assigned users.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, User Settings, and click Roles.

   The Role List page opens.

3. Check the Users column in the table to see the current usage of the role you intend to delete.

4. If any user accounts are using this role, remove the role assignment by taking the following steps:
   a. Select the role.
   b. Click Users.

      The User List page opens, filtered to show only users that are assigned to the selected role.
   c. Select the user account, and click Edit.
   d. Select another role from the Role list.
   e. Save the changes to the user account.
   f. Return to the Role List page.
5. Select the role that you want to delete.
6. Click Delete.

   The Delete Role page opens.
7. Click Delete to confirm the deletion.

   The role is removed from the list.

Product Privilege

The user account role is used to grant or restrict user access to CA Performance Center features, such as administration.

But individual data sources allocate product access differently. The 'product privilege' setting for data sources can be applied to create users with administrative capabilities. For example, a person can be a user of CA Performance Center, with no access to administration. That same person can have an Administrator product privilege to a specific instance of CA Network Flow Analysis. That person has full administrative privileges to that data source when following a drilldown path for a CA Network Flow Analysis managed item.

The following types of product privilege may be available in the data sources and synchronized to CA Performance Center:

Administrator

Performs all functions, including creating and editing SNMP profiles and other configuration.

Power User

Creates menus and dashboards. Can also edit and create roles.

User

Views menus and dashboards designated by an administrator or power user.

None

Has no access to a data source. This setting prevents the user from following a drilldown path from a view in CA Performance Center to the data source user interface. By default, all users have this product privilege setting for all data sources.

A user can be denied access to a particular data source while being given access to others.

CA Performance Center administrators can customize a user's access levels by selecting the appropriate role rights. For more information, see Role Rights (see page 95).

Coordinate the product privilege setting with the role rights settings. To follow a drilldown path to a data source, a user requires the appropriate role right and a product privilege for that data source.

The predefined administrator account, 'admin', has administrative privileges for any data sources that are registered. The predefined user account, 'user', has limited (user-level) privileges for those data sources.

Data Source Product Privileges

Each data source that is registered with CA Performance Center has its own product privilege with unique privileges within that interface. Administrators can assign a product privilege to a data source through CA Performance Center. The data source product privilege applies when users follow a drilldown path from a CA Performance Center data view to that particular data source. However, any privileges that are granted in this manner are specific to a data source instance. For example, if more than one CA Application Delivery Analysis data source is registered, the product privileges for each management console are managed separately.

The default administrator account, admin, is locked to prevent changes to product privileges. This account is required to have Administrator privileges for all registered data sources. Selecting a group of accounts that includes the admin account prevents you from editing the product privileges for any of the selected accounts.

CA Application Delivery Analysis Product Privileges

The following list summarizes product privileges applicable to the CA Application Delivery Analysis (formerly CA SuperAgent) management console:

A user must have product privileges on the CA Application Delivery Analysis data source to log in to the management console. Product privileges also specify access to the Administration page:

User

Gives access to all pages of the management console, except the Administration page.

Administrator

Gives access to all pages of the management console, including the Administration page.

Power User

Gives User-level product privilege, and Show Me menu access to the SNMP Profiles, Network Devices, and Device Groups on the Administration page.

Tip: If a user cannot log in to the management console user interface, verify that the user has been given a product privilege on the CA Application Delivery Analysis data source.

CA Network Flow Analysis Product Privileges

A user must have product privileges for the CA Network Flow Analysis data source to log in to the NFA console. Product privileges also determine whether a user can access the Administration page, and can perform certain functions:

Administrator

Gives access to the Administration page in the NFA console and to all functions. Functions include creating and managing user accounts, roles, groups, SNMP profiles, and scheduling for reports.

Power User

Gives user-level access and any additional abilities that the Role setting grants. For CA Network Flow Analysis, the Power User privilege is equivalent to the Administrator privilege.

User

Gives access to Top Interfaces reports and Interface Utilization reports on the Enterprise Overview page.

A User with the appropriate Permission Group settings also has access to the following reports:

- Top Hosts and Top Protocols reports on the Enterprise Overview page, if the user also has access to All Groups
- Interfaces page reports for the interfaces that are accessible to the user
- Existing reports on the Custom Reporting, Flow Forensics, and Analysis pages
- Menus that an administrator has assigned to the User role

The Role and Permission Group settings determine whether the User also can run existing reports, create reports, and manage reports. To create reports, a User must have access to All Groups.

None

Has no access to a data source. The user who has this product privilege cannot log in to the NFA console or drill down from a Performance Center view to the NFA console. By default, all users have this product privilege setting for all data sources.

Note: The same user account can have different privileges for different data sources.

CA Unified Communications Monitor Product Privileges

The following list summarizes the product privileges applicable to the CA Unified Communications Monitor management console:

Administrator

Gives access to all functions, including all administrative tasks: creating and editing Locations, media devices, thresholds, Call Watch definitions, incident responses, roles, and user accounts.

User

Gives access to report pages and to perform basic functions that the administrator selects. User permission does not provide access to administrative functions.

Manage Product Access

You allocate access to product features and data as you create each user account. You can use the following method to verify the role rights for a specific user. You can also change them if desired.

Follow these steps:

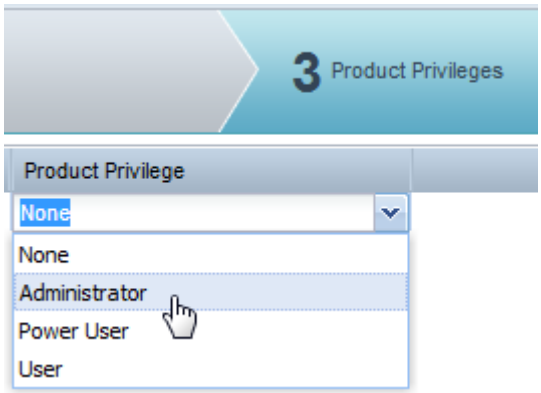
1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, User Settings, and click Users.

   The Manage Users page opens.
3. Select the user account that you want to edit.

   Note: The rights and privileges that are assigned to the predefined administrator account, 'admin', cannot be modified. This user account must have administrator access to all registered data sources.

   The Create New User wizard opens.
4. Click Product Privileges.

   All the data sources that are registered with CA Performance Center appear on the Product Privileges page.
5. Click the values that are shown in the Product Privileges column to enable drop-down lists.



   Each registered data source has a separate list.

6. Select one of the following product privileges from the drop-down lists:

   Administrator

   Performs all functions, including creating and editing groups, menus, dashboards, roles, and user accounts.

   Power User

   Creates menus and dashboards. Can also edit and create roles.

   User

   Views menus and dashboards that are designated by an administrator or power user.

   None

   Has no access to a data source. This setting prevents the user from following a drilldown path from a view in CA Performance Center to the data source user interface. By default, all users have this product privilege setting for all data sources.

7. Click Save.

   The changes to product privileges are saved to the selected user account.

Chapter 5: Creating and Managing User Accounts

This section contains the following topics:

User Accounts

Custom user accounts let operators view the data, menus, and dashboards that they require to perform their daily tasks. Operators with administrator role rights can create user accounts and manage existing accounts. Tenant administrators can manage user accounts only for their own tenant.

Before you create or edit user accounts, we recommend creating the custom groups and roles you require. Groups and roles are among the required parameters for each user account.

User Account Parameters

User accounts have the following required associations:

Role

The *role* is a parameter assigned to a user account that controls user access to product features and dashboard pages. Based on user job functions, the role grants administrative access to product configuration using *role rights*. Roles let users access data and product features that they require to perform their duties and restrict access to features that they do not require.

CA Performance Center provides multiple predefined roles, with different role rights. A user with the required role rights can create additional roles and assign them to user accounts.

Permission Groups

Permission groups comprise the scope of the managed items that each user can monitor. Administrators can create custom groups of managed items, such as applications, servers, networks, routers, and interfaces, to reflect each user's area of responsibility. When they are assigned to a user account as permissions, custom groups are called permission groups.

By default, new user accounts have no group assignment. If you want new users to see managed items, you must assign one or more groups to their user accounts. The predefined 'admin' and 'user' accounts have access to all groups. For user accounts that you create, limit the groups users can see based on their responsibilities.

Product Privilege

The *product privilege* is a type of permission set associated with a user account. The product privilege grants user access to features in selected data sources and does not apply to CA Performance Center functionality.

Note: In previous versions of NetQoS Performance Center, the product privilege referred to administrative access to product configuration, such as the ability to create custom groups. The role rights assigned to the user account now determine access to these features in CA Performance Center.

Predefined User Accounts

CA Performance Center provides two predefined ("factory") user accounts. These accounts are useful for performing initial setup. You can use them to allocate LDAP access with minimal role rights, or as templates for custom user accounts. But because they are common to all CA Performance Center installations, they are less secure.

Important! The factory user accounts are not substitutes for custom user accounts. We recommend changing the default passwords immediately after installation for improved security.

Note: You cannot delete the two predefined user accounts (**admin** and **user**).

The factory user accounts have the following parameters:

admin

Grants all administrative privileges.

Role: Administrator

Special Role Rights: All (the "global administrator" or Default Tenant administrator)

Permission Groups: Can view data from all groups

Default password: admin

user

Specifies typical operator privileges, such as viewing data.

Role: IT Operator

Special Role Rights: None

Permission Groups: Can view data from all groups

Default password: user

User account status is Enabled or Disabled. Disable an account to prevent a user from accessing the product.

Permission Groups and User Accounts

The predefined groups (or system groups) help you quickly organize performance data and allocate operator access to that data. However, a more secure and better managed system is based on custom groups that are assigned to users as permissions.

Permission groups comprise the scope of the managed items that each user can monitor. Administrators can create custom groups of managed items, such as applications, servers, networks, routers, and interfaces, to reflect each user's area of responsibility. When they are assigned to a user account as permissions, custom groups are called permission groups.

You can assign multiple permission groups to each user during user account creation. For example, assign the permission groups 'North American Core Routers' and 'North American Critical Applications' to the same user account.

Note: As a best practice, do not assign the 'Collections' group as part of a user's permission groups. This group should not be used for reporting.

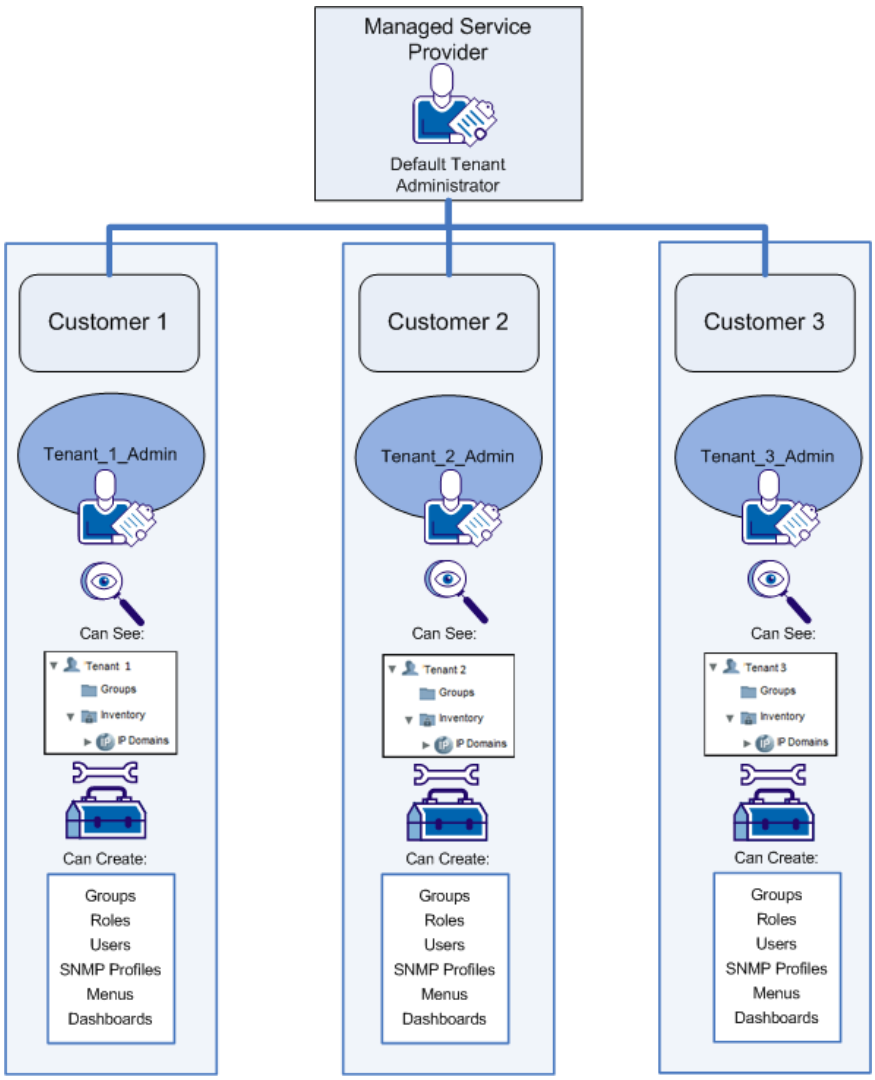
We recommend speaking with a CA technical representative to plan a strategy for creating a grouping and role structure. The best configuration meets your current requirements and is flexible enough to accommodate changes to your system.

Administrator Roles for Multi-Tenancy Support

When multi-tenancy is deployed, two distinct administrator roles are supported:

- Global Administrator - The Default Tenant administrator, usually representing an MSP. Product settings and data are not shared among tenants, but the Default Tenant Administrator can access them and modify all settings. This user must have the predefined "Administrator" role.
- Tenant Administrator - A limited administrator associated with a single tenant. This operator cannot access shared infrastructure or configuration belonging to the host (usually, the MSP). Tenant user accounts can include one or more of these administrator accounts.

When you create a tenant, the user interface prompts you to create a tenant administrator and a tenant user account. Operators who use these accounts can perform monitoring or administrative tasks within this tenant only. They cannot access the managed items and parameters associated with other tenants. Here is an illustration:



More information:

Add a Tenant (see page 130)
Predefined Roles (see page 90)
Administer a Tenant (see page 134)

How to Create a User Account

We recommend placing managed items in custom groups (see page 65) before creating user accounts. You assign custom groups to user accounts as "permission groups," which determine the data each user can view. And you can also grant selected ownership of a single branch of the Groups tree to a user account with administered groups.

Create any custom roles that you require before creating user accounts. Typically, the predefined roles (see page 90) provide starting points for customization.

We recommend the following process for creating a user account:

1. Log in as a user with the required administrative role rights (see page 95).
2. Confirm that the appropriate groups exist, or create them (see page 73) if necessary.

   Note: User account parameters include all of the groups that the user can *view*, and also one group that the user can *manage*. The Administer Groups role right (see page 95) lets users without full administrative rights manage a specific branch of the Groups tree.
3. Confirm that the appropriate roles exist, or create them if necessary.
4. Add a user, and enter basic user information (see page 121).
5. Assign a role.
6. Assign permission groups.

   Note: New user accounts have access to no groups by default. Their dashboards contain no data until you assign at least one permission group.
7. Assign group ownership so that the user can create and modify groups in one branch of the Groups tree.

   Note: Only user accounts with the Administer Groups role right are eligible for this selective group ownership.
8. Assign product privileges to grant access to the data sources you have registered.
9. Test the user account by temporarily proxying it.

More information:

User Account Parameters (see page 115)
Add a User Account (see page 121)

View a List of User Accounts

The Manage Users page lets you see high-level settings for user accounts. In a multi-tenant environment, the global administrator sees a list of user accounts that are not explicitly associated with a tenant. Tenant administrators only see user accounts for their tenant.

Before you create any custom user accounts, only the two factory user accounts are available.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Select Admin, User Settings, and click Users.

   The Manage Users page opens. This page displays the current list of user accounts.

   Note: Tenant administrators only see the items that are associated with their tenant.

   The table includes the following information about each user account:

   Name

   Is a login name for the user account.

   Role

   Is the role assigned to the user account.

   CAPC Privilege

   Identifies the level of access to data sources registered to CA Performance Center.

   Permission

   Lists the permission groups that are assigned to this account. Permission groups are shown as nested locations within the Groups tree. If this user is able to create custom groups that are not visible to other users, "My Custom Groups" are indicated.

   Default: '/All Groups'.

   Status

   Indicates whether the user account is enabled or disabled.

   To perform any action on this page, click one of the buttons along the bottom.

More information:

Role Rights (see page 95)
Predefined User Accounts (see page 116)
Add a User Account (see page 121)
Roles (see page 89)

Add a User Account

Add a user account for each person who will operate CA Performance Center. For security purposes, user accounts should not be shared.

Note: Before you create a user account, confirm that the required roles and groups exist.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the Manage Users page (see page 120).

   The page displays the current list of user accounts.
3. Click New.

   The Create New User wizard opens.
4. Enter information for the following account parameters:

   Name

   Is a login name for the user account. Limited to 50 characters.

   Description

   (Optional) Describes the user account to help you identify it.

   Preferred Language

   Specifies the language spoken by the operator associated with the user account.

   Email Address

   (Optional) Associates an email address with the user account.

   Authentication Type

   Identifies the authentication method that applies to this user account. The method must match Single Sign-On configuration. Select one of the following:

   - Performance Center—The default authentication scheme deployed by CA Performance Center.
   - External—A third-party authentication scheme, such as LDAP or SAML.

Password

Defines a password for the user account. The password is limited to 32 characters.

Time Zone

Corresponds to the time zone in which the user will view data.

Default: UTC (Coordinated Universal Time).

Role

Is the role assigned to the user account.

Account Status

Determines whether the account is enabled for use (activated).

5. Click Access Permissions to advance the wizard.
6. Add permission groups to the user account, as follows:
   - Expand the groups in the Available tree on the left.
   - Select a group or subgroup.
   - Click the right-pointing arrow to add your selection to the Selected area on the right.
   - Repeat as necessary.

   Note: As a best practice, do not assign the 'Collections' group as part of a user's permission groups. This group should not be used for reporting.
7. (Optional) Click the option to 'Enable My Custom Groups Functionality'.

   This option lets the user create custom groups to organize managed items for troubleshooting and analysis. These groups are only available to this user on the My Custom Groups page. They do not appear in the main Groups tree.

   A default group is selected for the user automatically. When the user logs in, data from the default group appears in dashboards by default.
8. (Optional) Select a different group from the 'Default Group' drop-down list.
9. Click Administer Group to advance the wizard. The Administer Group dialog lets you assign a group for a user with the role right of 'Administer Groups'.

10. Select a group for the user to administer, as follows:
    - Expand the groups in the Available Groups tree on the left.
    - Select a group or subgroup. The user has the ability to create groups *under* the selected group or subgroup, and then modify or delete only those administered groups. The user cannot modify or delete groups that are owned by another user. For more information about the 'Administer Group' role right, see Role Rights (see page 95).
    - Click the right-pointing arrow to add your selection to the Selected Group area on the right.

    Notes:
    - The Available Groups tree is filtered by the group selections on the Access Permissions dialog. This filtering prevents users from having administrative rights to a part of the tree from which they are prohibited.
    - The Administer Group dialog is disabled for users with the Administrator role.
11. Click Product Privileges to advance the wizard.
12. For each data source product in the Product list, select one of the following product privileges:

    Administrator

    Performs all functions, including creating and editing groups, menus, dashboards, roles, and user accounts.

    Power User

    Creates menus and dashboards. Can also edit and create roles.

    User

    Views menus and dashboards that are designated by an administrator or power user.

    None

    Has no access to a data source. This setting prevents the user from following a drilldown path from a view in CA Performance Center to the data source user interface. By default, all users have this product privilege setting for all data sources.

    Note: The same user account can have different privileges for different data sources.
13. Click Save.

    The new user account appears on the Manage Users page.

More information:

Permission Groups and User Accounts (see page 117)
Product Privilege (see page 108)
How to Create a User Account (see page 119)
Clone a Tenant (see page 132)

Chapter 6: Creating and Managing Tenants

This section contains the following topics:

About Tenants

By default, all managed items and their data are associated with the Default Tenant. Adding custom tenants to CA Performance Center lets you create separate CA Performance Center monitoring environments that you administer from a single user interface. A *tenant* represents a customer environment that a managed service provider administers. Each tenant environment is independent and effectively functions as a separate instance of CA Performance Center. Each instance can contain multiple users and roles that are not shared among tenants.

The basic tenant definition contains a few parameters to identify the MSP customer and let other operators access managed items and configuration for the customer. Each tenant must contain at least one IP domain. You or the tenant administrator can then set up as many of the following definitions as required to manage the enterprise infrastructure and applications:

- SNMP profiles
- Additional user accounts
- Roles
- Custom groups
- Custom dashboards
- Custom menus

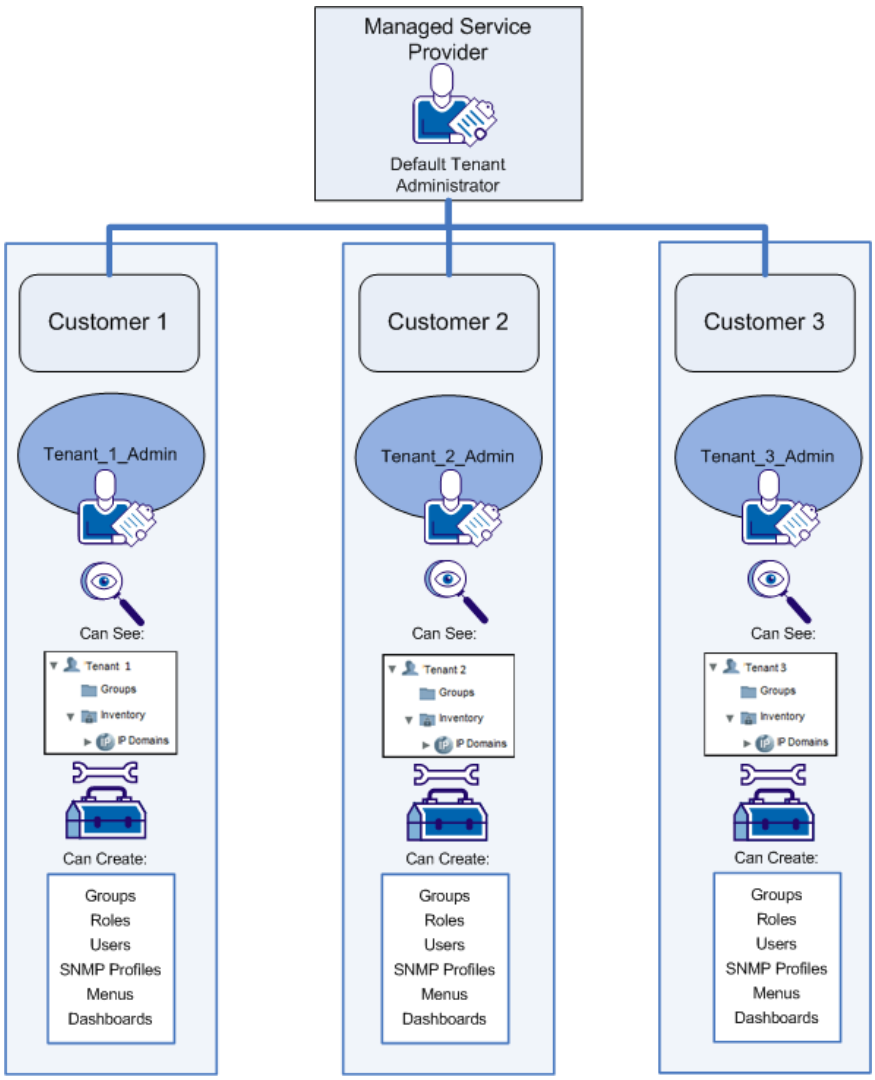
Custom IP domains (see page 37) provide the means of associating managed items with their tenants. A valid tenant definition contains at least one custom IP domain. As soon as a valid tenant exists in CA Performance Center, all items whose IP addresses match the tenant domain are associated with that tenant.

Administrator Roles for Multi-Tenancy Support

When multi-tenancy is deployed, two distinct administrator roles are supported:

- Global Administrator - The Default Tenant administrator, usually representing an MSP. Product settings and data are not shared among tenants, but the Default Tenant Administrator can access them and modify all settings. This user must have the predefined "Administrator" role.
- Tenant Administrator - A limited administrator associated with a single tenant. This operator cannot access shared infrastructure or configuration belonging to the host (usually, the MSP). Tenant user accounts can include one or more of these administrator accounts.

When you create a tenant, the user interface prompts you to create a tenant administrator and a tenant user account. Operators who use these accounts can perform monitoring or administrative tasks within this tenant only. They cannot access the managed items and parameters associated with other tenants. Here is an illustration:



More information:

Add a Tenant (see page 130)
Predefined Roles (see page 90)
Administer a Tenant (see page 134)

How to Deploy Multi-Tenancy

A user with the predefined Administrator role must perform the initial steps to create a multi-tenant environment in CA Performance Center. This predefined administrator account is called the "global" administrator and is associated with the Default Tenant space.

We recommend the following process for setting up a multi-tenant deployment:

1. Collect data about MSP customer virtual and physical systems.
2. Make a list of IP domains and SNMP versions, communities, or passwords for each MSP customer.
3. Create tenants. The tenant definition consists of a few simple parameters to identify the associated customer.

   The tenant definition also includes tenant administrator and user accounts.
4. Set the scope to a tenant to administer tenant configuration while logged in as a global administrator.
5. Create at least one IP domain to represent customer networks.
6. Create at least one SNMP profile to enable SNMP polling of devices supporting customer infrastructure.
7. Exit tenant administration. Repeat the previous steps for each tenant.

If data sources are already registered and collecting data, wait a few minutes. CA Performance Center creates system groups based on items that are discovered during monitoring. These groups are useful for creating custom groups that you can then allocate to users as permissions. See Groups (see page 61) for more information.

When system groups are available, take the following steps:

1. Set the scope to a tenant to administer tenant configuration, or log in as the tenant administrator.
2. Create any custom groups that are required to represent the customer networks and systems.
3. Edit the default tenant user account to add permission groups.

   Consider the likely role of this user and the managed items that this user manages.
4. Create any other custom roles, user accounts, SNMP profiles, dashboards, and menus that are required for this customer.

Work with each customer's IT staff to designate a user to act as the tenant administrator. The tenant administrator can complete the tenant configuration by creating custom groups and additional user accounts, if desired.

View a List of Tenants

Tenants are not required for all deployments. Create tenants to create separate CA Performance Center monitoring environments that you administer from a single user interface. The multi-tenancy feature lets an MSP monitor discrete customer networks and systems from a single instance of CA Performance Center. For more information, see About Tenants (see page 125).

The global administrator can use the Tenant List to see identifying information for all tenants.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Select Admin, Custom Settings, and click Tenants.

   The Manage Tenants page opens.

   The page displays the current list of tenants.

   If you have not created any custom tenants, only the predefined Default Tenant appears in the list.

   Important! This predefined tenant typically does not collect data in most data sources. Users who log in to this tenant probably do not see any data.

   Any custom tenants that you have created have values for the following parameters:

   Name

   Is a name for the tenant. Limited to 45 characters.

   Account ID

   Identifies this tenant; usually corresponds to the tenant account number or service tier with the MSP.

   Description

   (Optional) Describes the tenant.

   Status

   Is the status of this tenant. Select one of the following:

   - Enabled: Enables tenant user accounts for use.
   - Disabled: Prevents any actions by user accounts associated with this tenant.

Theme

Specifies the format—the theme that controls the appearance of the page in the browser window—to use for this tenant. All operators whose user account is associated with this tenant see this same theme.

Language

Specifies the language (locale) for this tenant. Select a language from the list.

To perform any action on this page, click one of the buttons along the bottom.

More information:

Add a Tenant (see page 130)
About Tenants (see page 125)
Set Tenant Scope (see page 135)
Administer a Tenant (see page 134)

Add a Tenant

Only a user with the predefined Administrator role (a "global" administrator) can add tenant definitions to distinguish among customer networks and systems. This user is equivalent to the tenant administrator for the Default Tenant.

During tenant creation, you can also create a tenant administrator and a tenant user. Unlike the global administrator, the tenant administrator can only see data and configuration for a single tenant. Data from other MSP customers is not accessible to a tenant administrator.

To add multiple tenants rapidly, use the Clone Tenant (see page 132) feature.

Follow these steps:

1. Log in as a user with the predefined (global) Administrator role.

   Note: A tenant administrator cannot create tenants.

2. Navigate to the Manage Tenants page (see page 129).

   The page displays the current list of tenants.

3. Click New.

   The Add New Tenant page opens.

4. Supply the required information and make selections in the fields provided:

   Name

   Is a name for the tenant.

   Account ID

   Identifies this tenant; usually corresponds to the MSP account number.

   Description

   (Optional) Describes the tenant.

   Status

   Is the status of this tenant. Select one of the following options:

   - Enabled: Enables tenant user accounts for use.
   - Disabled: Prevents any actions by user accounts that are associated with this tenant.

   Theme

   Specifies the format—the theme that controls the appearance of the page in the browser window—to use for this tenant. All operators whose user account is associated with this tenant see this same theme.

   Language

   Specifies the language (locale) for this tenant. Select a language from the list.

5. Create the tenant administrator account for this tenant. Enter information for the following parameters:

   Administrator

   Is a login name for the tenant administrator account.

   Password

   Defines a password for the user account. The password is limited to 32 characters.

   Confirm Password

   Confirms the password.

6. Create the tenant user account. The associated operator can access tenant-specific dashboards, but cannot access any administration functions.

7. Click Save.

   The new tenant definition is created, but it lacks required parameters, such as IP domains. For more information, see Set Tenant Scope (see page 135).

More information:

Clone a Tenant (see page 132)
Administrator Roles for Multi-Tenancy Support (see page 117)

Edit a Tenant

The global administrator can modify tenant definitions that have already been created.

When you modify a tenant definition, the changes do not affect the monitoring definitions that are associated with that tenant. To modify the SNMP profiles, IP domains, or other configuration for a tenant, you must either log in as a tenant administrator or set the tenant scope to administer the tenant. For more information, see Administer a Tenant (see page 134).

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Tenants page (see page 129).

   The page displays the current list of tenants.
3. Select a tenant definition in the list and click Edit.

   The Edit Tenant page opens.
4. Modify tenant parameters (see page 130) as required.
5. Click Save.

   The changes to the tenant definition are saved. The new values appear in the Tenant List.

Clone a Tenant

The fastest way to create multiple tenants with similar parameters is by using the Clone Tenant feature. You can select a tenant definition that you have already created and "clone" it, changing parameters for the resulting new definitions where required.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Tenants page (see page 129).

   The page displays the current list of tenants.
3. Select the tenant definition that you want to clone, and click Clone.

   The Clone Tenant page opens.

4. Supply the required information in the fields provided. By default, basic parameters are cloned except for the Name and Account ID parameters.

   Name

   Is a name for the tenant. Limited to 45 characters.

   Account ID

   Identifies this tenant; usually corresponds to the tenant account number or service tier with the MSP.

5. Type a username and password for the tenant administrator account.
6. Type a username and password for the tenant user account.
7. Click Save.

   A new tenant definition is created, based on the cloned tenant definition. However, it lacks required parameters, such as IP domains. You must now set up the tenant environment. For more information, see Setting Up Tenants (see page 133).

Setting Up Tenants

The topic Add a Tenant (see page 130) explains how to create a basic tenant. However, the basic definition is not useful until you set up the required monitoring parameters and user access.

You can set up a tenant environment by logging in as a tenant administrator associated with that tenant. Or, if you are a global administrator, you can use the Administer Tenant feature to access CA Performance Center from the perspective of the tenant.

When you set the tenant scope to a selected tenant, you see only the configuration items available to that tenant. You can then administer the tenant, creating the required IP domains, user accounts, and more. They will only be available to users with permission to see the items that belong to that tenant.

More information:

Add a Tenant (see page 130)
Set Tenant Scope (see page 135)
Administer a Tenant (see page 134)
Administrator Roles for Multi-Tenancy Support (see page 117)

Administer a Tenant

The global administrator or a tenant administrator has the necessary permissions to modify the monitoring parameters that belong to a tenant. Custom definitions that you create while administering a tenant are specific to that tenant and not shared among tenants.

To modify the IP domain, SNMP profile, user, role, and group definitions for a tenant, the tenant administrator simply logs in. The global administrator (the administrator for the Default Tenant) must set the tenant scope to the selected tenant to gain access to these definitions.

Note: The global administrator can create tenant administrator user accounts for each tenant.

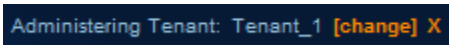
When the tenant scope has been set, the procedures for administering a tenant are identical to the procedures to perform in a single-tenant environment.

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 135) to access tenant configuration while logged in as the global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

   You can now see and modify only definitions associated with this tenant.

2. Click the Admin tab, and select an item to modify:
   - IP Domains
   - SNMP Profiles
   - Groups
   - Menus
   - Roles
   - Users
3. Follow the procedures specific to the selected item.
4. Save your changes.

   The modifications are only apparent to administrators and to operators whose user accounts were created within this tenant environment.

More information:

Set Up Tenant IP Domains (see page 136)
Set Up Tenant Roles (see page 139)
Set Up Tenant Users (see page 142)
Set Up Tenant Groups (see page 137)
Set Up Tenant SNMP Profiles (see page 137)
Set Up Tenant Menus (see page 144)

Set Tenant Scope

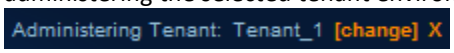
Set up the environment for a tenant that you have already created by using the Administer Tenant feature. For example, you can add custom IP domains, user accounts, or groups to the tenant. Set the scope to the tenant to access CA Performance Center from the perspective of the tenant.

Follow these steps:

1. Log in as a user with the predefined Administrator role (a "global" administrator).
2. Navigate to the Manage Tenants page (see page 129).

   The page displays the current list of tenants.
3. Select the tenant that you want to administer.
4. Click Administer.

   The Administering Tenant indicator appears at the top right to show that you are administering the selected tenant environment.

   You are only able to see the configuration associated with the selected tenant.

   You can now create the IP domains, SNMP profiles, roles, users, menus, and groups that are required to represent and monitor this tenant environment. Use the menus under the Admin tab to configure the tenant.
5. (Optional) Change the tenant scope to another tenant by clicking the [change] link next to the Administering Tenant indicator.

   You return to the Manage Tenants page, where you can select another tenant.
6. Exit a tenant scope by clicking the X next to the tenant indicator.

Set Up Tenant IP Domains

Tenant definitions are created and configured as separate steps. A tenant definition must contain at least one IP domain that identifies the IP addresses of managed items in the tenant environment.

After you create a tenant definition, add all IP domains containing the tenant's managed devices.

Data sources classify managed items into IP domains using different methods. Typically, domain identifiers do not appear in the data source until you have created at least one custom domain in CA Performance Center.

Follow these steps:

1. Log in as a tenant administrator for the selected tenant.

   Or set the tenant scope (see page 135) to access tenant configuration as a global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, Custom Settings, and click IP Domains.

   The Manage IP Domains for [Tenant Name] page opens.

3. Click New.

   The IP Domains Administration dialog opens.

4. Supply information for the required parameters (see page 40).

5. Click Save.

   The new IP domain appears in the list, which is scoped to the current tenant.

   Repeat the steps as required to add more domains to this tenant.

Set Up Tenant SNMP Profiles

A tenant definition can contain one or multiple SNMP profiles, which are used to contact devices in the tenant enterprise systems using SNMP. Operators who are logged into one of the tenant user accounts only have permission to view the SNMP profiles that were created for that tenant.

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 135) to access tenant configuration while logged in as a global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, User Settings, and click SNMP Profiles.

   The Manage SNMP Profiles for [Tenant Name] page opens.

3. Click New.

   The Add SNMP Profile dialog opens.

4. Complete the required fields (see page 31) and change any default settings as needed. Some fields display only when SNMPv3 is selected.

5. Click Save.

   You return to the Manage SNMP Profiles for [Tenant Name] page.

   The new profile appears in the SNMP Profile List, which is scoped for the current tenant.

Set Up Tenant Groups

The groups that you create while administering a tenant are specific to that tenant. Custom groups are not shared among tenants. Create groups that reflect the unique virtual and physical systems of each tenant in a multi-tenant monitoring environment.

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 135) to access tenant configuration while logged in as a global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, User Settings, and click Groups.

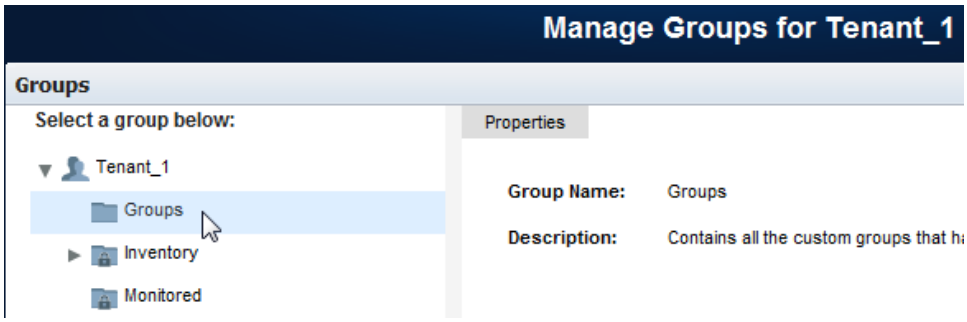
   The Manage Groups for [Tenant Name] page opens.

   When scoped to a tenant, the top-level node in the Groups tree is a system group (see page 63) automatically created for the tenant. You can add subgroups to this group, but it cannot otherwise be modified.

   The Groups tree contains nodes for tenant IP domains and Service Provider nodes for system groups that are shared among tenants at the discretion of the global administrator. The Service Provider groups are read-only to tenant administrators.

3. Expand the Tenants node in the Groups tree.

4. Place the new group in the tenant subgroup named Groups.



5. Click Add Group.

   The Add Group dialog opens. The New tab is selected by default.

6. Supply values for the following parameters:

   Group Name

   Specifies a name for the group. Do not use the following special characters in group names: /&\,%.

   Description

   (Optional) Helps you identify the group.

7. Confirm the setting for the following parameter:

   Include the children of managed items

   Adds the children of managed items automatically when the items are added to this group. If you disable this option and add a router to the group, the interfaces on that router are not included. Therefore, their data is not visible in drilldown views.

   Default: Selected.

8. Select either Custom or Site from the Group Type list.

9. Click Save.

   The new group appears in the Groups tree under Tenant\Groups. Users who are associated with this tenant only see groups and items in this section. They have no access to groups or items associated with other tenant domains.

   The group contains no items until you add them. You have two options for adding items to a custom group:

   - Manually populate the group (see page 81) by adding items in the Manage Groups interface.
   - Create rules (see page 76) to manage group membership

Set Up Tenant Roles

Tenants are created and configured as separate steps. A tenant definition can contain one or multiple user account roles. Custom tenant roles are useful for specific requirements, such as a user who can search the Inventory and can drill down into data sources but can only view dashboards within a single tenant.

The operator who logs in with each tenant role only has permission to view data from managed items that belong to that tenant.

Users with the predefined Administrator role can also create tenant administrator roles, which grant the ability to:

- Add tenant user accounts
- Create custom tenant groups
- Create custom tenant dashboards

Unlike the global administrator, a tenant administrator does not have access to data or Admin features in any other tenant environment. For more information, see Roles for Multi-Tenancy Support (see page 117).

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 135) to access tenant configuration as a global administrator.

   The tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, User Settings, and click Roles.

   The Manage Roles for [Tenant Name] page opens.

3. Click New.

   The Add Role for [Tenant Name] page opens.

4. Supply the required information and make selections in the fields provided.

   Name

   Is a name for the new role. Limited to 45 characters.

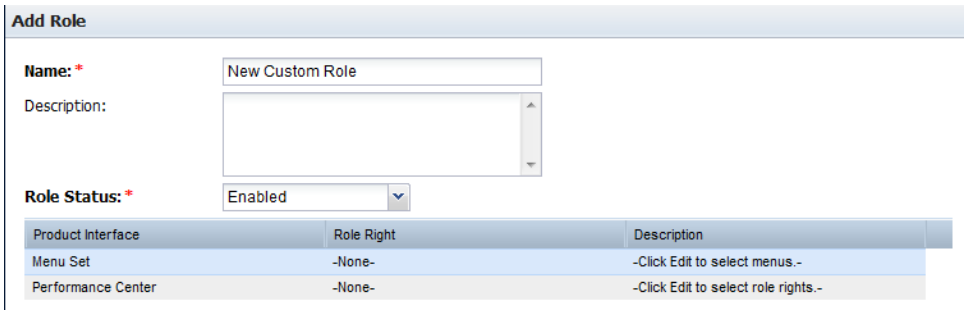
   Description

   (Optional) Describes the new role.

   Role Status

   Lets you enable the role to make it active. The role must be enabled to give users with this role the appropriate rights.

   A table indicates that no role rights have been selected for the role.



5. Select Menu Set, and click Edit.

   The Edit Menu Set dialog opens, where you can select menus for this role. Menus listed in the 'Available Menus' area can be added to the role.

6. Click an item on the left that you want to add to the role, and then click the right arrow.

   The selected item moves to the Selected Menus list.

   Use Shift + Click or Ctrl + Click to select multiple items in the list.

7. (Optional) Use the Up and Down arrows to move items around in the list. The order of menus in the list determines their order on the Dashboards tab.

8. Click Save.

   You return to the Add Role page.

9. Select CA Performance Center, and click Edit.

   The Edit Role Rights dialog opens, where you can select individual access rights for this role.

10. Click an item that you want to add to the role, and then click the right arrow to move it to the Selected Rights list.

    Use Shift + Click or Ctrl + Click to select multiple items in the list.

11. (Optional) Use the Up and Down arrows to move items around in the list. The order of role rights determines their priority in cases where rights overlap.

12. Click Save.

    You return to the Add Role page.

13. Click Save.

    The new role appears in the Role List, which is scoped for the current tenant.

More information:

Add a Role (see page 104)
Role Rights (see page 95)
User Account Parameters (see page 115)
Add a User Account (see page 121)

Set Up Tenant Users

A tenant definition can contain one or multiple user accounts. The operator who is associated with each user account only has permission to view data from managed items that belong to that tenant.

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 135) to access tenant configuration while logged in as a global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, User Settings, and click Users.

   The Manage Users for [Tenant Name] page opens.

   The page displays the current list of user accounts for this tenant.

3. Click New.

   The Create New User wizard opens.

4. Enter information for the required account parameters:

   Name

   Is a login name for the user account. Limited to 50 characters.

   Description

   (Optional) Describes the user account to help you identify it.

   Email Address

   (Optional) Associates an email address with the user account.

   Preferred Language

   Specifies the language spoken by the operator associated with the user account.

   Authentication Type

   Identifies the authentication method that applies to this user account. The method must match Single Sign-On configuration. Select one of the following:

   - Performance Center—The default authentication scheme deployed by CA Performance Center.
   - External—A third-party authentication scheme, such as LDAP or SAML.

   Password

   Defines a password for the user account. The password is limited to 32 characters.

   Time Zone

   Corresponds to the time zone in which the user will view data.

   Default: UTC (Coordinated Universal Time).

   Role

   Is the role assigned to the user account.

   Account Status

   Determines whether the account is enabled for use (activated).

   Other account parameters do not apply to user accounts that are scoped to a tenant.

5. Click Save.

   The new user account is saved as part of the tenant definition. Any operator who logs in with this user account only sees dashboards and data from managed items in the IP domains associated with this tenant.

Set Up Tenant Menus

Menus determine how dashboards are organized on a per-user basis. Create menus that correspond to the roles of IT staff members who use CA Performance Center to monitor the physical and virtual systems of each tenant.

Important! The steps for administering tenant menus and dashboards are slightly different than the steps for performing other tenant configuration. After you set the tenant scope, you must also proxy a tenant administrator to create menus.

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 135) to access tenant configuration as a global administrator, and then proxy a tenant administrator associated with this tenant.

2. Select Admin, User Settings, and click Menus.

   The Manage Menus for [Tenant Name] page opens.

   The page displays the current list of menus for this tenant.

3. Click New.

   The Add Menu page opens.

4. Type a Name for the menu. This name appears in the floating menu when you click the Dashboards tab.

5. (Optional) Type a Description of the menu to help other operators identify it.

6. Select a dashboard in the Available Dashboards list.

7. Click the right arrow.

   The dashboard moves to the Selected Dashboards list.

   Use Shift + Click or Ctrl + Click to select multiple dashboards. Use the up and down arrows to change the order of the dashboards in the menu.

   Note: A maximum of 20 dashboards can be assigned to a single menu. An error message appears if you try to add more than 20 dashboards.

8. Click Save to save the new menu. Or click Save and Add Another to create more menus.

   When users associated with this tenant log in, they see the new menu on the Dashboards tab. Users associated with other tenants do not see it.

Delete a Tenant

Only a global administrator can delete a tenant definition. Tenant administrators do not have this ability.

Deleting a tenant definition removes all of the associated definitions for that tenant, including all of the following:

- Data sources
- SNMP profiles
- IP domains
- User accounts
- Roles
- Groups
- Custom dashboards
- Custom menus

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Tenants page (see page 129).

   The page displays the current list of tenants.
3. Select the tenant definition that you want to delete, and click Delete.

   You are asked to confirm the operation.
4. Click Yes to confirm the deletion.

   The tenant definition is deleted. It no longer appears in the Tenant List.

Chapter 7: Logs and Troubleshooting

This section contains the following topics:

Logs

By checking your log files daily or weekly, you can resolve problems before they affect normal operations. All logs are stored in subfolders that correspond to a service (or daemon). Find log files in the following path:

`CA/PerformanceCenter/`*`servicename`*`/logs`

Replace the *servicename* parameter with one of the following service names:

DM

The Device Manager.

- DMService.log – Output from the Device Manager, primarily related to synchronization.
- wrapper.log – caperfcenter_devicemanager process logging.

EM

The Event Manager.

- EMService.log – Output from the Event Manager; includes details of events and alarms.
- wrapper.log – caperfcenter_eventmanager process logging.

PC

The main console program.

- PCService.log – CA Performance Center-related logging; comprises user interface and view components.
- wrapper.log – caperfcenter_console process logging.

SSO

The Single Sign-On authentication software.

- SSOService.log – Single Sign-On logging, including HTTPS (Secure Sockets Layer) information where HTTPS has been configured.
- wrapper.log – caperfcenter_sso process logging.

For problems with the Single Sign-On Configuration Tool, check the application log in the following location:

`/opt/CA/PerformanceCenter/sso/logs/application.log`

Log filenames include the relevant date and time.

New log files are generated automatically each day. Older log files are removed automatically after 14 days to avoid consuming excessive disk space.

Access the most recent log file to find errors associated with the database or data source synchronization. You can start by opening the Events dashboard from the Dashboards tab and sorting by Status. If you want to look at the related log file, note the event type and failure date and time. In the log directory, open the log file with the corresponding date in the filename.

Set Logging Levels

By default, CA Performance Center log files contain only high-level information about errors and warnings about your monitoring system. For more advanced troubleshooting situations, you can change the logging level so that more information is collected and written to the daily log files.

Follow these steps:

1. In the Linux command-line interface on the CA Performance Center appliance, log in as root.
2. Navigate to the following directory for the service whose logging levels you want to change. See Logs (see page 147) for a list of options for the *servicename* parameter.

   `/opt/CA/PerformanceCenter/servicename/etc/`
3. Open the log configuration file named log4j.xml.
4. To change the global logging level, locate the **<root>** element.

5. Change the **<priority value>** in the **<root>** element to one of the following logging levels:
   - FATAL, which identifies severe error events that can cause an application to fail.
   - ERROR, which identifies error events that are serious, but probably allow an application to continue running.
   - WARN, which identifies potentially harmful situations.
   - INFO, which provides informational messages about the progress of an application.
   - DEBUG, which provides information that is useful for debugging a problem.
6. To change the logging level for a specific log, locate the relevant **<logger>** element.
7. Change the value of the logger level to one of the values listed in Step 5.

Search Multiple Log Files

If you have access to the CA Performance Center server, you can search multiple log files simultaneously. Searching multiple files lets you find all instances of a specific type of error. Look for log files for each component in the relevant subdirectory. For example, look for the Device Manager log in the "DM" subfolder.

Follow these steps:

1. In the Linux command-line interface on the CA Performance Center appliance, log in as root.
2. Navigate to the logs directory for the service whose logs you want to search. See Logs (see page 147) for a list of options for the *servicename* parameter.

   ```
   opt/CA/PerformanceCenter/servicename/logs
   ```
3. Enter the following command:

   ```
   grep -i keyword *
   ```
4. Substitute any of the following for *keyword*:
   - “error”
   - “warn”
   - “failed”
   - “no data”

   A list of log files containing the keyword is returned.
5. Use a text editor program on the local server to view the log files.

Data Source Registration Failed

Symptom:

I attempted to add a new data source, but the registration failed.

A message stated, 'Create Data Source Failed: Data source communication failure.'

Solution:

This message indicates that the data source is unreachable. Do the following:

- Verify that the data source is running.
- Verify that the DNS hostname or IP address of the server where the data source database is installed is correct. You can edit the data source to view this information.
- Check intervening firewalls. Make sure they are configured to let CA Performance Center communications reach the data sources. For more information about the ports to open, see the *Installation Guide*.

Solution:

If the failure occurred with a CA Infrastructure Management Data Aggregator data source, verify that it is running. Access the following URL:

```
http://<host>:<port_number>/rest
```

where 'host' is the IP address of the server where the Data Aggregator is installed, and 'port_number' is the port used to access the RESTful web service, usually 8181.

The web service status indicates whether the Data Aggregator is running.

Solution:

Check the Device Manager application.log file. The file is written to the following directory:

```
CA\PerformanceCenter\PC\logs
```

The log entry references the URI used by CA Performance Center to communicate with the data source, along with a stack trace.

Data Source Synchronization Failed

Symptom:

When I tried to perform a data source synchronization, I saw a 'Synchronization failure' message.

Solution:

A synchronization failure might indicate that the data source is unreachable. Do the following:

- Verify that the data source is running.
- Verify that the DNS hostname or IP address of the server where the data source database is installed is correct on the Add Data Source page.

Solution:

A synchronization failure can indicate that the data source could not handle the data sent to it during synchronization.

First, check the Data Source Log for the data source. For more information, see View the Data Source Log (see page 24).

If you still cannot determine the source of the problem, check the Device Manager application.log file. It is written to the following directory:

```
CA\PerformanceCenter\PC\logs
```

If the data source was unable to handle data received from CA Performance Center during synchronization, the log entry shows a general SOAP exception.

Solution:

CA Performance Center encountered an issue during the attempted synchronization.

Check the log files, as instructed above. Look for an exception and stack trace within the following phases of synchronization:

- Pull
- Global Sync
- Bind (only executes when initially synchronizing with a data source)
- Push

The log contains detailed information about the steps that are performed during each phase. This information can help pinpoint the cause for the synchronization failure.

Solution:

System times are not synchronized. Check the NTP server or the system time on each server (including data sources and the CA Performance Center server).

More information:

View the Data Source Log (see page 24)
Synchronization (see page 21)
Data Source Registration Failed (see page 150)

Data Source Test Failed

Symptom:

I tested a data source during the registration process, but the test failed.

Solution:

Do the following:

- Verify that the DNS hostname or IP address of the server where the database for the data source is installed is correct.
- Attempt the data source registration anyway. The data source registration might succeed even if the test failed.
- Check the logs for registration failure information. For more information, see Data Source Registration Failed (see page 150).

Solution:

If the failure occurred with a CA Infrastructure Management Data Aggregator data source, verify that it is running. Access the following URL:

```
http://<host>:<portnumber>/rest
```

where 'host' is the IP address of the server where the Data Aggregator is installed, and 'portnumber' is the port used to access the RESTful web service, usually 8181.

Note: This URL does not call up the correct page in Mozilla Firefox. Use another supported browser.

The web service status indicates whether the Data Aggregator is running.

Solution:

If the failure occurred with a data source other than a CA Infrastructure Management Data Aggregator, check the application log file (PC/logs/application.log) for a corresponding event. The log entry includes the URI that CA Performance Center used to communicate with the data source, as well as a stack trace.

More information:

Register a Data Source (see page 25)

Inventory is Empty

Symptom:

I have installed a data source and registered it, but now I do not see any managed items in the Inventory.

Solution:

Check to make sure the data source is registered and has an active status. Do the following:

1. Log in as a user with administrative privileges.
2. Select Admin, Data Source Settings, and click Data Sources.

   The Manage Data Sources page opens. The list shows each registered data source, along with its status.

Solution:

One of the following might have occurred:

- Data source registration failed. For more information, see Data Source Registration Failed (see page 150).
- Data source synchronization failed. For more information, see Data Source Synchronization Failed (see page 150).

Solution:

Check the permissions for the user account that you used to log in. If the user account has no assigned permission groups, you see no managed items. For more information, see Add a User Account (see page 121).

Also make sure that you have not logged in as a user associated with the Default Tenant. This tenant typically sees no managed items.

Data Is Missing from Views

Symptom:

Some interface views are missing some data; some of the table columns are empty. For example, interface and device names, interface speeds, and utilization data is missing from views.

Solution:

Some data sources do not support authentication passwords or privacy passwords that fall below a minimum length.

SNMP profiles that use the SNMPv3 format let you enable authentication and privacy options. When you create an SNMPv3 profile, specify an authentication password that is eight characters or more in length. If you specify a shorter authentication password, the password and SNMP profile are invalid. These profiles may not be successful in communicating with devices. In this case, SNMP data are missing for the affected interfaces.

Similarly, blank passwords are not supported for SNMP v3 profiles with MD5 or SHA as the Authentication Protocol.

Solution:

Edit the SNMPv3 profile, and supply an authentication password that is eight characters or more in length.

More information:

Add an SNMP Profile (see page 31)

'No Data' Message in Views

Symptom:

Several views on the dashboard are empty. A message states, "No Data to Display".

Solution:

A graph or table view on a dashboard can show "No Data to Display" for many reasons, such as the following:

- The data source for the view has not been installed or has not been registered.

  Each view receives data from a single data source. Some view containers appear on dashboards even if the corresponding data source is not registered. They are always empty until the data source is registered.

  You can change display settings so that such views are never displayed in dashboards. For more information, see Disable View Suppression (see page 16).

  Tip: You can often determine which data source is associated with the view by clicking the ? button on the view.

- The data source is registered, but it has been temporarily disabled.

  A disabled data source is not polled for data. An administrator can edit the data source to enable it. For more information, see Register a Data Source (see page 25).

- The view type requires editing before data can be displayed.

  Some types of view do not have default settings. For example, multiviews and multitrend views require customization before they display any data.

- No data is available for the selected time range. To test this theory, select a different time range.
- Not enough time has transpired since polling started on the devices that are selected for reporting.

  If the polling interval is fairly long, the first data point can take a little longer to appear. Polling rates are set in the data sources.
- A service is not running.

  If the device manager service is not running, you are likely to see the "no data" message. Instructions for checking the status of a CA Performance Center daemon are provided in the *Installation Guide.*
- The current group does not contain items of the required type for this view.

  The group of items whose data is reported on the dashboard is shown above the Time Period selector. Check the view: is this Server report trying to show data from a group of routers?
- The group is new or has recently been changed.

  Check group membership. A group rule might be misconfigured.

  If your user account has the required role right, edit the view to select another group context. Or click the Group Filter link above the Time Period selector and select another group context for the dashboard.
- The user account of the logged-in user does not have permission to view monitored items that have reported data. For more information, see How to Create a User Account (see page 119).
- The data source has not properly synchronized with CA Performance Center. For more information, see Data Source Synchronization Failed (see page 150).
- Components were not discovered, or managed item discovery failed.

  This problem is data source-specific, so consult the online Help for the data source. For a Data Aggregator data source, you can check inventory discovery history. On the Discovery Profiles List page, select the Discovery profile that you created for the initial discovery and click the History button.
- Metric families were not configured or enabled.

  A Data Aggregator data source automatically applies predefined (factory) monitoring profiles to the predefined collections, such as the All Routers collection. However, custom groups and custom collections are subject to misconfigured custom monitoring profiles.
- The database query timed out. Network connectivity issues between the CA Performance Center server and the data source can cause this problem.

NetQoS--NPC--Troubleshooting--No Charts or Images are Visible

Symptom:

Some charts or images do not appear in CA Performance Center. A red X appears to indicate that the chart or image is broken.

Solution:

You are using the secure HTTP (HTTPS) when running CA Performance Center in Internet Explorer (IE). In IE, the Transport Layer Security (TLS) setting needed for HTTPS is set to only TLS 1.0 by default. To view the broken charts or missing images, turn on TLS 1.1.

Follow these steps:

1. Click Tools at the top of the browser, or click the gear icon at the top right.
2. Click Internet Options.
3. Click the Advanced tab, and select the TLS 1.1 checkbox.
4. Click Apply.

   The TLS settings are saved.

Using CA Remote Engineer

The CA Remote Engineer (CARE) tool gathers data that a CA Support Engineer can use to help you troubleshoot a problem. CARE contains configuration files in its scripts directory for every product that CARE supports

CARE is installed when you install CA Infrastructure Management components:

Component	Installation Directory
CA Performance Center	/opt/CA/PerformanceCenter/RemoteEngineer
Data Aggregator	/opt/IMDataAggregator/RemoteEngineer
Data Collector	/opt/IMDataCollector/RemoteEngineer

Data Repository	The Data Repository installer extracts CARE to the /opt/CA/IMDataRepository_vertica7 directory. Run **dr_install.sh** to copy CARE to each node in the cluster in the /opt/CA/RemoteEngineer directory.

When prompted by a CA Support Engineer, take the following steps to run CARE to collect troubleshooting data.

Follow these steps:

1. At a command prompt, navigate to your installation directory:

   `cd install dir`

2. Enter the following command:

   `./re.sh`

3. When prompted, enter one of the following, depending on where you are running CARE:
   - CAPC
   - IMDataAggregator
   - IMDataCollector
   - IMDataRepository
4. When asked whether you want to FTP the CARE files to CA Support, provide one of the following responses:
   - **y** The CARE files are sent to CA Support.
   - **n** The CARE files are saved in a ZIP file that you can manually deliver to CA Support.

Chapter 8: Working with Dashboards and Reports

This section contains the following topics:

Viewing Data in CA Performance Center

Dashboard pages display dynamic views of data that CA Performance Center receives, interprets, and formats from registered data sources. *Views*, or *data views*, present statistical data, usually in a graph or table format. Each view represents a discrete set of collected data. Depending on your user account role rights, you can add and edit individual views or remove them from a dashboard page. In some cases, you can export the data to a file in CSV format.

View placement on dashboard pages is flexible. Users with the required role rights can customize dashboards. They can, for example, place views of application performance data next to views of volume data to help troubleshoot issues from a single page.

The predefined dashboards are organized into workflows. Hyperlinks let you drill down from Top N views to more detailed metrics from a narrow context, such as an individual device. Built-in workflows direct you to data that is related to the metric you are reviewing. For example, you can see a view of discards when you drill down from a view of interface utilization.

Create custom groups to display data for a specific set of sites, devices, or interfaces. You can apply these groups to dashboards using the group selector (the 'change' link at the top left). You can change the “context” of the dashboard to analyze data for specific groupings. You can also select a managed item or a group of items and rapidly generate an on-demand report (see page 177) for a selected metric family and time frame.

Views that show data for a group contain rollups of data from data sources. Views of data for a single managed item often provide a drilldown path directly to the data source. The Single Sign-On feature lets you navigate from a dashboard to a data source interface if your user account has the 'Drill into Data Sources' role right.

More information:

Dashboards and Reports (see page 170)

Context Page Navigation

You can frequently access more information about individual managed items from dashboards. Most dashboards are composed of views of summary data, such as hourly rollups or averages from a group of items. If additional data is available from the data source, you can click linked items on the dashboard page to drill down into *context pages*.

Note: The role right to Drill into Views is required.

The views on context pages show filtered data from a narrow context, such as a view of data from a single managed item. Use the links to drill down into specific data and home in on the source of a performance problem.

In data views from some data sources, you can also right-click the name of an item in a table view to access a menu. For example, right-click the link that corresponds to an item name in the Inventory section. A menu lets you select a related context page, containing more granular data.

Finally, some context pages include tabs to additional pages of detailed data. Click a tab to see data that has been filtered by a selected managed item or type of item.

Device Name Display

Users with the predefined Administrator role can define aliases for device names. The alias is then displayed, where appropriate, in CA Performance Center views.

A device alias is a user-configured name that is applied to the associated managed item in CA Performance Center. If an alias is not defined, the discovered device name is displayed. If the alias is used, you can still view the discovered names on the Details tab of the Interface or Device Context pages.

Interface Description Display

The interface description is displayed, where appropriate, in CA Performance Center views. For example, the list of interfaces in the Inventory and the list of interface addresses in the Inventory contains a Description column. In interface views, the interface description is displayed as follows:

- If a view contains a subtitle, the interface description is included in it.
- If a view contains a Name column but the view does *not* contain a Description column, the interface description is appended to the interface name in the Name column.
- The interface description is appended to the interface name in any views where the description is not displayed already.

Inventory of Managed Items

The Inventory page is available from the Inventory tab. The Inventory contains a list of all items that all data sources discover and monitor, called *managed items*. Managed items of all types, such as applications, devices, or interfaces, appear in list views on Inventory pages. Use the Inventory to create on-demand reports (see page 177).

A 'Consoles' section of the page contains a list of links to any registered data sources with separate consoles. The necessary product privilege to each data source is required for access.

The Inventory list shows only categories of items currently available to CA Performance Center from the registered data sources. Further, it only displays items that are members of the groups in your user account permission set. The categories are links that let you access filtered lists that show all managed items of the selected type.

The list pages provide minimal information to identify each item, such as device hostnames or IP addresses. Select a check box to enable on-demand reporting for a managed item.

If multiple data sources monitor a single managed item, CA Performance Center reconciles its identity and creates a single item in the Inventory.

More information:

Performing Searches (see page 161)
Inventory is Empty (see page 153)

Performing Searches

Some deployments scale to hundreds of thousands of managed items. Multiple search features help you locate data for specific items or groups of items.

If your user account has the required role right, you can begin your search from the Inventory tab. On this tab, you can view a list of managed item types. Click a link to see a list of items. Then search among the items themselves in the list using the search field and the sorting and paging features below the list view.

Inventory and Search Results pages also provide access to on-demand reports (see page 177).

Note: The ability to view the Inventory and perform a global search is granted to individual operators with their role. Only users with the 'View Inventory and Search' role right can view the Inventory tab.

Perform a global search using the search field at the top of any page. This type of search scans all items in the database, across all data sources. A global search returns lists of all items in the Inventory that match your search, sorted by item type. Filtering the results further is also supported in each view. For more information, see Narrowing a Search with Filters (see page 163).

A more limited search feature is available for table views and does not require a special role right. The search that you perform from a table footer filters out managed items that would otherwise appear in that view. No items from other views or dashboards are displayed.

Search for a Managed Item

You can navigate directly to contextual information about a single item, such as a router that seems to be associated with a network issue. Search fields for data views let you search for items within selected views. You can search on dashboard pages and, if your user account has the required role rights, on Admin and Inventory pages.

Follow these steps:

1. Navigate to a dashboard or inventory page where you want to begin your search.

   Note: If you have the required role rights, you can also search in the Admin pages, including in the Groups tree on the Manage Groups page.

2. Enter a search string in the search field, and click Enter.

   You can supply a text string, a search string containing numbers, or a combination of both.

   Note: Wildcard characters are accepted in this field, such as an asterisk (*) for a multicharacter match.

   For more information, see Narrowing a Search with Filters (see page 163).

   The search results appear within categories of similar items.

3. Click one of the items in the list.

   A Context page that contains information about the selected item opens.

Narrowing a Search with Filters

You can narrow or broaden the searches that you perform by adding a wildcard character or filter text to the Search field. Filters can be applied to a global search or to a view-level search.

You can use an asterisk (*) as a wildcard character in your searches. For example:

- “serv*” returns all the rows with entries starting with “serv”.
- “*erver” returns all the rows with entries ending in “erver”.
- “*server*” is the same as “server” and returns all the words that contain the word “server” - such as my_server, or server1, or just server.
- “ser*ver” finds all the words that start with “ser” and end with “ver” including “server”.

You can add multiple search words to narrow the search further. For example, if you search for devices using the search string “server 192.168*”, the search returns all servers on the 192.168.0.0/16 network.

If your environment contains many managed items, such as 4 million servers, we recommend filtering global searches. Otherwise, a limit on each global search preserves user interface performance.

Set Alias Names For Multiple Monitored Devices

CA Performance Center includes a script to set aliases for multiple monitored devices. You can use this script to set the aliases for more than one monitored device at a time. The alias appears in the inventory list of devices and in the inventory list of interfaces.

Note: An alias that is set using this script takes precedence over the alias that you can set by importing a CSV file when you add an IP domain. For information on importing a CSV file, see the *CA Performance Center Administrator Guide*.

This script has two functions. First, the script returns a list of device item IDs and device names in .csv format. You modify the .csv file to include the alias names that you want to set on each monitored device. The second function of the script is to take the updated .csv file and set the alias names for the monitored devices.

Follow these steps:

1. Open a command prompt and access the *Performance_Center_installation_directory*/PerformanceCenter/Tools/bin directory.

2. To call the script to set alias names for monitored devices, type the following command:

   `./update_alias_name.sh`

   The script parameters are listed and are described.

3. To return a complete list of monitored devices, type the following command:

   `./update_alias_name.sh -h host_name -u username -p password [-T item_type] [-o output_filename]`

   -h *host_name*

   Specifies the CA Performance Center host name to connect to.

   -u *username*

   Specifies the username of the CA Performance Center administrator who is to set the alias names.

   -p *password*

   Specifies the password for the CA Performance Center administrator who is to set the alias names.

   -T *item_type*

   Specifies the type of item that you want to set alias names for. Valid values are device, interface, or component.

   Default: device

   Keep the default value.

   -o *output_filename*

   (Optional) Creates a .csv file with the total number of monitored devices by itemID and Device Name with a different filename for the .csv file than the default filename. If you do not enter a value for this parameter, the default name, DeviceList.csv, is used for the .csv file.

   The .csv file has the following format: Device ItemID, Device Name.

   For example:

   560, MyRouter1

   561, MyRouter2

4. Modify the .csv file that was created in the previous step, noting the alias name that you want to set for each monitored device. This file must have the following format: Device ItemID, Device Alias Name.

   Note: if the Item IDs in your .csv file are invalid, no error messages appear. These invalid entries are ignored.

For example:

560, MyRouter1AliasDisplayName

561, MyRouter2AliasDisplayName

Note: Commas and spaces are allowed in the Alias Name field of the .csv file.

5. Type the following command:

   `./update_alias_name.sh -h host_name -u username -p password [-T device] -i input_file`

   -i *input_file*

   Specifies the filename of the .csv file that you created previously with the alias names.

   The alias names are set for monitored devices.

   Note: If -i is not specified, the script looks up all of the item IDs that are required for the specified type, and creates a csv file with item IDs and item names.

6. (Optional) To set alias names for a large number of monitored devices, type the following command to adjust the batch size and pause between batches. These adjustments help to control the workload:

   `./update_alias_name.sh -h host_name -u username -p password -T device -i input_file -b batch_size –t time_in_seconds`

   –b *batch_size*

   Indicates the number of items to process in each batch.

   Default: 10000

   Default if the -i parameter is not specified: 150

   –t *time_in_seconds*

   Indicates the time, in seconds, to pause between batches.

   Default: 1

   Default if the -i parameter is not specified: 1

   For example:

   `./update_alias_name.sh -h host_name -u username -p password -T device -i input_file -b 20 –t 2`

More information:

Add an IP Domain (see page 40)

Set Alias Names For Interfaces and Components Across Multiple Monitored Devices

CA Performance Center includes a script to set alias names for interfaces and components across multiple monitored devices. Users see the alias names in the inventory list of interfaces and in dashboards and views, depending on the role rights you assign.

This script has two functions. First, the script returns a list of interface item IDs or component item IDs, and interface names or component names in .csv format. You modify the .csv file to include the alias names that you want to set for interfaces or components. The second function of the script is to take the updated .csv file and set the alias names for the interfaces or components.

Follow these steps:

1. Open a command prompt and access the *Performance_Center_installation_directory*/PerformanceCenter/Tools/bin directory.
2. To call the script to set alias names for interfaces and components, type the following command:

   `./update_alias_name.sh`

   The script parameters are listed and are described.

Example: Set Alias Names for Interfaces

1. To return a complete list of interfaces that a Data Aggregator host is monitoring, type the following command:

   `./update_alias_name.sh -h host_name -u username -p password -T item_type [-o output_filename]`

   -h *host_name*

   Specifies the CA Performance Center host name to connect to.

   -u *username*

   Specifies the username of the CA Performance Center administrator who is to set the alias names.

   -p *password*

   Specifies the password for the CA Performance Center administrator who is to set the alias names.

-T *item_type*

Specifies the type of item that you want to set alias names for. Valid values are device, interface, or component.

Default: device

Specify interface.

-o *output_filename*

(Optional) Creates a .csv file with the total number of interfaces by Device Item ID, Interface Item ID, and Interface Name with a different filename for the .csv file than the default filename. If you do not enter a value for this parameter, the default name, InterfaceList.csv, is used for the .csv file.

The .csv file has the following format: Device Item ID, Interface Item ID, Interface Name.

For example:

560, 164, MyInterface1

561, 165, MyInterface2

2. Modify the .csv file that was created in the previous step, noting the alias name that you want to set for each interface. This file must have the following format: Device Item ID, Interface Item ID, Interface Alias Name.

   Note: if the Item IDs in your .csv file are invalid, no error messages appear. These invalid entries are ignored.

   For example:

   560 , 164, MyInterface1AliasDisplayName

   561, 165, MyInterface2AliasDisplayName

   Note: Commas and spaces are allowed in the Alias Name field of the .csv file.

3. Type the following command:

   `./update_alias_name.sh -h host_name -u username -p password -T interface -i input_file`

   -i *input_file*

   Specifies the filename of the .csv file that you created previously with the alias names.

   The alias names are set for interfaces.

   Note: If -i is not specified, the script looks up all of the item IDs that are required for the specified type, and creates a csv file with item IDs and item names.

4. (Optional) To set alias names for a large number of interfaces, type the following command to adjust the batch size and pause between batches. These adjustments help to control the workload:

   `./update_alias_name.sh -h host_name -u username -p password -T interface -i input_file -b batch_size –t time_in_seconds`

   –b *batch_size*

   Indicates the number of items to process in each batch.

   Default: 10000

   Default if the -i parameter is not specified: 150

   –t *time_in_seconds*

   Indicates the time, in seconds, to pause between batches.

   Default: 1

   Default if the -i parameter is not specified: 1

   For example:

   `./update_alias_name.sh -h host_name -u username -p password -T interface -i input_file -b 20 –t 2`

Example: Set Alias Names for Components

1. To return a complete list of components that a Data Aggregator host is monitoring, type the following command:

   `./update_alias_name.sh -h host_name -u username -p password -T item_type [-o output_filename]`

   -h *host_name*

   Specifies the CA Performance Center host name to connect to.

   -u *username*

   Specifies the username of the CA Performance Center administrator who is to set the alias names.

   -p *password*

   Specifies the password for the CA Performance Center administrator who is to set the alias names.

   -T *item_type*

   Specifies the type of item that you want to set alias names for. Valid values are device, interface, or component.

   Default: device

   Specify component.

-o *output_filename*

(Optional) Creates a .csv file with the total number of components by Device Item ID, Component Item ID, and Component Name, with a different filename for the .csv file than the default filename. If you do not enter a value for this parameter, the default name, ComponentList.csv, is used for the .csv file.

The .csv file has the following format: Device Item ID, Component Item ID, Component Name.

For example:

565, 166, MyComponent1

566, 167, MyComponent2

2. Modify the .csv file that was created in the previous step, noting the alias name that you want to set for each component. This file must have the following format: Device Item ID, Component Item ID, Component Alias Name.

   Note: if the Item IDs in your .csv file are invalid, no error messages appear. These invalid entries are ignored.

   For example:

   565 , 166, MyComponent1AliasDisplayName

   566, 167, MyComponent2AliasDisplayName

   Note: Commas and spaces are allowed in the Alias Name field of the .csv file.

3. Type the following command:

   `./update_alias_name.sh -h host_name -u username -p password -T component -i input_file`

   -i *input_file*

   Specifies the filename of the .csv file that you created previously with the alias names.

   The alias names are set for components.

4. (Optional) To set alias names for a large number of components, type the following command to adjust the batch size and pause between batches. These adjustments help to control the workload:

   `./update_alias_name.sh -h host_name -T component -i input_file -b batch_size –t time_in_seconds`

   –b *batch_size*

   Indicates the number of items to process in each batch.

   Default: 10000

   Default if the -i parameter is not specified: 150

–t ***time_in_seconds***

Indicates the time, in seconds, to pause between batches.

Default: 1

Default if the -i parameter is not specified: 1

For example:

```
./update_alias_name.sh -h host_name -u username -p password -T component -i
input_file -b 20 –t 2
```

More information:

Add an IP Domain (see page 40)

Dashboards and Reports

Dashboards are dynamic report-building pages within the CA Performance Center user interface. They appear as menu items that are accessible from the Dashboards tab. Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

Note: Your user account role rights determine the dashboards that you can see.

Reports are static output from an on-demand selection or an exported dashboard page. Reports that you export from a dashboard create a static data set from the data and information in the associated dashboard. On-demand reports capture a data set from a single managed item or group in the Inventory. You can print reports, send them by email, or export them in CSV or PDF format. For each format, the report captures a selected data set.

Dashboards are organized in menus. *Menus* are segments of the Dashboards tab that are used to organize dashboards by their content. By default, Administrators and Designers can customize menus and assign them to user account roles.

CA Performance Center offers a set of factory dashboards and menus, which are available for use immediately after registering data sources. Users with the required role rights can also extensively customize dashboards, menus, and views to create a custom system for individual operators.

The menus and dashboards that are available to you are displayed when you hover over or click the Dashboards tab.

More information:

On-Demand Reports (see page 177)

Types of Report Pages

Two categories of dashboards are available by default or through customization:

- *Summary pages* provide high-level information, such as averages from groups of managed items. Summary dashboards often provide a drilldown path to more detailed, related pages from a selected context.
- *Context pages* provide specific, focused performance or status data from a narrow context, such as a single router or server. These pages are available as drill-down links or tabs from Summary dashboards.

To drill in to a detailed view from a Summary dashboard, take one of the following steps:

- Right-click the item to select the context page that you want to see.
- Click the item to open the default context page.

Note: Your role rights (see page 95) must include the ability to Drill into Views.

Default sets of context pages are available for individual devices, interfaces, and servers. These pages include a set of customizable tabs that let you access more specific context data for a selected managed item. For example, the Router context includes tabs for Health, Utilization, and Error data.

Set a Dashboard as Your Home Page

By default, CA Performance Center opens to one of the following dashboards when you log in:

- The first dashboard in your list of 'My Dashboards'
- The Infrastructure Overview dashboard (the out-of-the-box default)

You can set a different dashboard, a *home page*, to open when you log in. You can easily return to this home page from another location in the CA Performance Center console.

Follow these steps:

1. Navigate to the dashboard that you want to set as your home page.
2. (*Optional*) Click the [change] link to set the group context for the dashboard. The home page remembers this context.
3. Click More, Set as Home Page.
4. In the confirmation dialog, click Yes.

   The selected dashboard is now your home page.
5. To return to your home page from another location in the console, click the CA logo in the upper left of the console window.

Notes:

- When the group associated with the dashboard is removed from your permission set, your default permission group is used for the home page.
- When you log on or click the CA logo, an error message tells you if views on the dashboard are suppressed.

Modify a Context Page

Context pages provide specific, focused performance or status data from a narrow context, such as a single router or server. These pages are available as drill-down links or tabs from Summary dashboards.

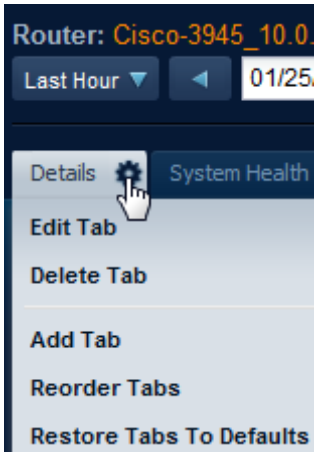
You can customize context pages if your user account has the 'Edit Context Pages' and 'Drill into Views' role rights. The predefined Administrator and Designer roles have these role rights by default.

You can add or remove the tabbed pages that contain data views in context pages. You can edit the predefined tabs and can change the views that are displayed on those tabs. You can also rearrange tabs to change their order. Select 'Restore Tabs to Defaults' to revert changes to all tabs in the current context. All modifications are saved to the current tenant.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 95).
2. Navigate to the item context whose page you want to edit. For example, click the link for a router on any dashboard to call up the Router context pages. Or navigate directly to an item context by clicking the item on an Inventory page.

   The first tab on the left is selected by default. The tab that is selected includes an Edit icon to let you access the Edit menu.



3. Click Edit.
4. Select from the following options:

   Edit tab

   Lets you select new views for the selected tab (see page 174) and change the item context for the views.

   Delete tab

   Lets you delete a tab that you select from a list.

   Important! No Undo or Restore feature is available. Any tab that you delete must be restored manually if required.

   Add tab

   Lets you access options to create a tab.

   Reorder tabs

   Lets you move the existing tabs into different positions relative to each other.

More information:

Add or Edit a Context Page (see page 174)
Create a Context Tab (see page 175)
Rearrange Context Tabs (see page 176)

Add or Edit a Context Page

You can customize context pages if your user account has the 'Edit Context Pages' and 'Drill into Views' role rights. The predefined Administrator and Designer roles have these role rights by default.

Unlike standard dashboard pages, item context pages are clustered in sets of tabbed pages. You can edit the predefined tabs and can change the views that are displayed on those tabs. You can add tabbed pages. You can also rearrange the tabs in an item context to change their order. Revert changes to all tabs in the current context by selecting 'Restore Tabs to Defaults' from the Edit Tab menu.

Modifications apply to the current tenant.

Follow these steps:

1. Log in as a user with the required role rights (see page 95).
2. Navigate to the item context whose page you want to edit. For example, click the link for a router on any dashboard to call up the Router context pages.

   The tab that is selected includes an Edit icon to let you access the Edit menu.
3. Select the tab that you want to modify.

   The Edit icon appears.
4. Click the Edit icon, and select Add or Edit tab.
5. (Optional) Select one of the Default Tab Templates from the menu. Each template populates the page with the default views for that type of page.
6. Change the Tab Title. A title is required.

   The tab title determines the name that appears at the top of the tabbed context page.

7. Select a layout template for the page from the Layout buttons.
8. Remove unwanted views from the page if desired. In the Layout pane, click:
   - Clear Layout to change the positioning of all views on the page.
   - An [X] to remove an individual view from the page.

   The views that are available to be added to the page are shown in categorized lists. The lists are filtered by the selected group or item context.

   All registered data sources are represented. However, the available views are limited to those views that are applicable to the context.

   Note: You cannot change the item context for the page; it is preselected for the present context.
9. Click to expand the categories of views.
10. Select a view, drag it to the Layout pane, and drop it where you want it to appear.
11. Click Save.

    The context page refreshes to reflect your changes. The changes persist across login sessions, but they are only applied to the current tenant.

Create a Context Tab

You can create context pages if your user account has the 'Edit Context Pages' and 'Drill into Views' role rights. The predefined Administrator and Designer roles have these role rights by default.

Note: The 'Create a Dashboard' role right is not required to create a context tab.

Unlike standard dashboard pages, item context pages are clustered in sets of tabbed pages. When you add a context tab, a new tabbed page is displayed in the item context. Only users associated with the current tenant can see the new tab.

Follow these steps:

1. Log in as a user with the required role rights (see page 95).
2. Navigate to the item context where you plan to add a page. For example, click the link for a router on any dashboard to call up the Router context pages.

   The first tab on the left is selected by default. The tab that is selected includes an Edit icon to let you access the Edit menu.
3. Click the Edit icon, and select Add tab.
4. Change the Tab Title if desired.

   The tab title determines the name that appears at the top of the tabbed context page.

5. Select a layout template for the page from the Layout buttons.
6. Remove unwanted views from the page if desired. In the Layout pane, click:
   - Clear Layout to change the positioning of all views on the page.
   - An [X] to remove an individual view from the page.

   The views that are available to be added to the page are shown in categorized lists. The lists are filtered by the selected group or item context.

   All registered data sources are represented.

   Note: You cannot change the item context for the page; it is preselected for the present context.
7. Click to expand the categories of views.
8. Select a view, drag it to the Layout pane, and drop it where you want it to appear.
9. Click Save.

   The context page refreshes to include the new tab. The changes persist across login sessions.

Rearrange Context Tabs

You can customize context pages if your user account has the 'Edit Context Pages' and 'Drill into Views' role rights. The predefined Administrator and Designer roles have these role rights by default.

Each item context consists of sets of tabbed pages. In addition to modifying individual tabbed pages, you can rearrange the tabs in an item context to change their order. Modifications are only saved to the current tenant.

Follow these steps:

1. Log in as a user with the required role rights (see page 95).
2. Navigate to the item context whose page you want to edit. For example, click the link for a router on any dashboard to call up the Router context pages.

   The tab that is selected includes an Edit icon to let you access the Edit menu. By default, the first tab on the left is selected.
3. Click the Edit icon, and select Reorder tabs.

   The Reorder Tabs dialog displays a list of Current Context Page Tabs.

   The list reflects the current ordering of tabs, from left to right.
4. Select a tab to move, and drag it to another location in the list.

5. Click Save.

   The context page refreshes to reflect your changes. The tabs are displayed in a new order from left to right.

   If too many tabs are available for the context to display without horizontal scrolling, an arrow appears on the right. Click the arrow to see additional tabs.

On-Demand Reports

Quickly view metrics for selected groups, devices, or interfaces using the on-demand feature. On-demand trend reporting is useful for close investigation of a targeted managed item or for groups of items.

Access on-demand reports from an Inventory page, from a page of search results, or from the Manage On-Demand Report Templates page (see page 181).

The Inventory and search pages only display items that are included in your user account permission groups. Select a managed item for the trend report, and click On Demand. You can then select settings for the report, such as additional items, metrics, and a chart format.

Note: The ability to view the Inventory and perform a global search is granted to individual operators with their role. Only users with the 'View Inventory and Search' role right can view the Inventory tab. As a result, this role right (see page 95) is required to enable on-demand reporting.

When you have generated the on-demand trend report, you can then select an output format to share the results with coworkers. Role rights to print reports and send them by email are required to enable sharing.

Generate an On-Demand Report

Users with any role can generate on-demand trend reports to view a static data set from a narrow context. Use on-demand reports for close investigations and troubleshooting.

You can start from the Inventory pages or from a page of search results to generate an on-demand report.

Follow these steps:

1. Select the Inventory tab, and click an item type, such as Devices.
2. Locate the managed item that you plan to include in the report. Or perform a search for the item and locate it in the results.

3. Select the check box next to the item, and click On Demand.

   A settings dialog opens.

   Important: Use the scroll bar on the right of the dialog to view all settings options.

4. (Optional) Change the default view title. The title appears on the view, which in turn appears in the report.

5. Supply a name for the on-demand report. The name identifies the report in the On-Demand Report Templates list and appears as a title for the report.

6. (Optional) Supply a description for the report to identify it.

7. Select a View Type option. These options determine the chart format. Select from the following options:

   - **Chart with Multiple Metrics**: This view consists of one chart that displays a trend line for each metric that you selected.
   - **Chart per Metric**: This view consists of one chart for each metric that you selected. Each chart displays a trend line for the metric.
   - **Chart per Item with Multiple Metrics**: This view consists of one chart for each item or group that you selected. Each chart then displays trend lines for each metric that you selected.
   - **Chart per Metric with Multiple Items**: This view consists of one chart for each metric that you selected. Each chart then displays trend lines for every item or group that you selected.

   For more information about the View Type options, see On-Demand Report Options (see page 180).

8. Select a Resolution option.

   The Resolution is the amount of time that each data point in a chart represents.

9. (Optional) Select different managed items to include in the report. Take the following steps:

   a. Click Add Items.

   b. Click Add/Remove Items.

      (Optional) A dialog lets you change the Context Type.

      Note: After you make initial selections, changing the item context can clear the original selections. For more information, see On-Demand Report Options (see page 180).

c. Select managed items from the list, and then click Add. Add up to 15 items.

Note: Only the managed items that are included in your permission groups are displayed.

The items that you selected appear in the Selected [Items] pane.

d. Click OK to return to the View Settings dialog.

The items that you selected appear in the list of Items to Include. Only these items are queried for performance data.

10. (Optional) Select a group to include in the report. Take the following steps:

a. Click Add Groups.

b. Click Add/Remove Groups to display the Groups tree. The dialog is filtered to show only groups that are included in your permission groups.

c. Click to expand nodes in the Groups tree.

d. Click to select a group, then click the right arrow to move it to the Selected Groups pane. You can add up to 15 groups.

Note: To remove an item or group, click the Add/Remove button to return to the Add/Remove Items or Groups dialog. Select the item or group in the Selected pane, and click Remove.

Important: You cannot include any groups that are in the Collections category. The Collections groups are not currently available for inclusion in reports.

11. Click OK.

12. (Optional) In the Metric Calculate Level pane, select how to calculate the aggregated data: by Group, by Device, or by Component. These options are available when you select 'Chart per Item with Multiple Metrics' or 'Chart per Metric with Multiple Items' from the View Type field.

13. Select the metrics to display in the report. Take the following steps:

a. Click to expand the folders in the Available Metrics pane. Each folder represents a metric family. For example, select the 'CPU' metric family to see the available CPU statistics.

b. Click to select individual metrics. Select up to 15 metrics.

Note: Only the metrics that apply to the selected item are available in the list.

c. Click the arrow to move your selections to the Selected Metrics pane.

14. Select the scope of your changes from the Apply Changes drop-down. Select one of the following options:
    - My User Account: Saves the report exclusively to your user account.
    - For All Tenant Users: Saves the report so that it is only available to users associated with your tenant (possibly the Default Tenant).

    Note: The availability of these options depends on your user account role rights.
15. (Optional) Click the Run button to preview your report.

    A preview dashboard displays the view format that you have selected.
16. Click the Save link on the toolbar on the preview page to save the report template.

    The Settings dialog opens to let you make more changes before saving.

    Once saved, a report template appears in a list on the Manage On-Demand Report Templates page.
17. Export the report by clicking Print, Email, or the Edit icon (to export to CSV).

On-Demand Report Options

When you create an on-demand report template, multiple options let you select the number and appearance of charts in the generated report.

View Options determine how the on-demand report displays data. As you configure the report, you can select multiple items or a single group for reporting. View options determine how charts represent all metric families that you select, from all of the selected managed items or groups. Group rollup data is represented by aggregated trend lines.

The following options are available:

- **Chart with Multiple Metrics**: This view consists of one chart that displays a trend line for each metric that you selected. Different colors are used to distinguish the trend lines.
- **Chart per Metric**: This view consists of one chart for each metric that you selected. Each chart displays a trend line for the metric.
- **Chart per Item with Multiple Metrics**: This view consists of one chart for each item or group that you selected. Each chart then displays trend lines for every metric that you selected.

  Some metric families automatically report on multiple device components. For example, a CPU metric family reports data from all CPUs that are detected on a managed device. In these cases, a separate chart is created for each CPU.
- **Chart per Metric with Multiple Items**: This view consists of one chart for each metric that you selected. Each chart then displays trend lines for each item or group that you selected.

Note: Groups are represented as individual items for reporting. The data is rolled up from all managed items in each group.

Take care to select managed items and metric families that complement each other. After you make initial selections, changing the item context can clear the original selections. For example, if you select three routers for reporting and then add interfaces, the routers are cleared. The report reflects interface data, but no rollups to the router level.

Other device types and components are compatible for reporting in a single on-demand report, however. For example, routers and servers can be included in the same report.

Also keep in mind the amount of processing that is required for certain combinations of options. Groups with a large number of managed items require a great deal of processing, particularly if you then select an option that requires a chart for each item. This situation is exacerbated when you also select component metrics for reporting, such as CPU or memory. For example, you are reporting on a group that contains 200 routers, and you select 'Chart per Item with Multiple Metrics' as the View Type. If you then select CPU metrics from the list of Metrics to Include and change the 'Metric Calculate Level' to 'by Component,' , the view sends queries to Data Aggregator for CPU data from every CPU in every router in this group. And then 200 charts must be rendered for the report to be fully generated.

View the List of Report Templates

The Manage On-Demand Report Templates page provides a list of reusable report definitions. No predefined reports are provided; if you have not created any on-demand reports, the list is empty.

Once you create some on-demand reports, the list displays key features of each report template. Click New to create an on-demand report.

By default, you can see, generate, and modify the reports that you created, as well as reports that were created within your tenant. Click My Reports to filter the list so that only the reports that you created are displayed.

Follow these steps:

1. Log in as a user with either the Administer Reports or Run Reports role right (see page 95).
2. Select Reports, and click On-Demand Report Templates.

   The Manage On-Demand Report Templates page opens.

   The page displays the current list of reports. If no on-demand reports have been created, the list is empty.

The following information is listed for each report:

Name

Identifies the report (the title that you supplied).

Description

Describes the report.

Creation Date

Shows the date and time when the report was generated.

Last Modified

Shows the date and time when the report was last edited.

Owner

Indicates the username of the user account that owns the report template (the creator of the on-demand report). The permissions of this user are enforced when the report is either modified or generated by another user. Only the owner can delete a report template.

If no tenants have been created, the reports in the list are visible to all users. The global administrator sees a list of reports that are not explicitly associated with a tenant (that is, they are associated with the Default Tenant). Tenant administrators only see the items that are associated with their tenant.

More information:

Generate an On-Demand Report (see page 177)

View Options

Many views offer a search feature and other settings that you can change to modify the view. In addition to filtering and time frame options, the following options are available for most data views:

- Editing view settings  , such as changing its title or severity categories.
- Seeing more data by selecting another "page" of a table view.
- Increasing or decreasing the number of items that are shown per "page".
- Collapsing the view so that the data is hidden.
- Changing the managed item context for the data shown in the view.

  Note: Users with the 'Save Changes to Shared Views' role right (see page 95) can save view modifications to their own user account. The changes persist after logout. However, other users cannot see changes to views.

Other view options are specific to the selected view. The available options depend on the format and data source.

Trend View Options

The trend views that are available in context pages let you quickly and easily change the trend lines that are displayed on the graph. The following options also apply to multitrend views:

- Right-click a metric in the chart legend and select Hide to remove it from the view.
- Exclude all other metrics by right-clicking a metric in the legend and selecting Focus.
- Narrow the focus to a precise time frame using the zoom feature.

Trend views also include an option to add a "goal line" as a visual indication of performance levels or thresholds. You can supply any value or label for the goal line, and you can show or hide the goal line for a selected trend view.

Table View Options

In table views, you can drill down to detailed data for individual items. Use the page feature to see metrics from a longer list of items. Increase the Max Per Page value to increase the size of the view and the number of table rows per page.

You can sort table data columns by selected metrics and also select columns to include. Click a table column to sort. A white arrow on the column lets you access a menu of table column options. Select Columns to enable and disable the metrics that were enabled for the table by default.

Browser View Options

The *browser view* is a unique view type that lets you add a URL to a selected report page. You can use this view to compare external factors alongside your network performance views. Also, the browser view lets you update internal and external data dynamically. The URL must be for a web page that supports embedded iframes.

Multiple external factors can affect the performance of your network and servers, such as world events and adverse weather conditions. The ability to view a weather map and news headlines alongside performance data views on a single report page can help you better understand patterns in network performance.

Device Admin Option

When a view does not display Data Aggregator data, this option lets you drill down directly to the Data Aggregator Admin page to troubleshoot monitored devices and items.