CA Performance Center

Administrator Guide

2.1.0.0

CA Technologies Product References

This document references the following CA Technologies products:

- 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
- 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 6: Creating and Managing Tenants 113

Chapter 7: Working with Dashboards 131

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 that was collected by network and systems-monitoring products. You can compare large amounts of statistical data from multiple sources within a single 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. It 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 adding supported data sources (data source *registration*). However, you can make other customizations to suit your environment and make reporting more useful.

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

1. Plan group structure and naming conventions. For more information, see Creating and Managing Groups (see page 87).

   (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 113).

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 53) and Creating and Managing Roles (see page 65).

3. List the dashboards and menus suitable for each role. For more information, see Organizing Dashboards in Menus (see page 149).

4. Register data sources. For more information, see Register a Data Source (see page 22).

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 28).

7. Create groups of managed items. For more information, see Create a New Group (see page 99).
8. Create roles, and assign menus to roles. For more information, see Add a Role (see page 77).
9. Create user accounts, and assign roles and permission groups to these accounts. For more information, see Add a User Account (see page 59).
10. Create menus containing dashboards for reporting. For more information, see Add a Menu (see page 151).
11. (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 (see page 64).
12. (Optional) Create tenants to represent all customer enterprises. For more information, see Add a Tenant (see page 116).
13. (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).

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 70).
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) 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.

6. (Optional) Enable SSL encryption. This parameter is required if you want to use a secure connection to send email from CA Performance Center.

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 so that it uses a logo you select.

Themes are typically applied per tenant. You customize a theme and assign that theme to a tenant. The custom logo appears in the header of reports (in PDF format) that tenant users print or send by email. If you are not deploying multi-tenancy, the theme applies to the default tenant, which is transparent to you.

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.

   If the image does not meet the criteria, you see a message explaining the requirements that were not met. You can then modify the image and upload it again.

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 must be square. Use a 1:1 aspect ratio. If necessary, surround the logo with a square background.
- The image must be in one of the following file formats:
  - .bmp
  - .gif
  - .png
  - .jpg
- (Optional) The image background should be transparent or white.
- (Optional) The image should have 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.

Managing Data Sources

Data sources are the supported products that provide performance and configuration data to CA Performance Center. Data source products, which perform monitoring, data collection, and data aggregation, can often function independently. However, once they are registered to an instance of CA Performance Center, they are called 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 additional management. If you set up SSL encryption in your environment, you must edit data source connection parameters. A data source log (see page 22) 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 22)
Edit a Data Source (see page 24)
Synchronize a Data Source (see page 21)

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. It 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 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 additional data sources are registered.

Multiple user accounts might share a username in different data sources. But some account parameters might differ. Manual editing is required in this situation. For example, assume that you have a user 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 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

When you register a data source that contains SNMP profile definitions, those profiles are automatically added 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 duplication of these parameters is detected, CA Performance Center retains the profile whose timestamp indicates the most recent modification.

If a duplicate Profile Name is synchronized but the User or Community String values do not match, CA Performance Center saves the new profile, appending a number to the name. For example, the first profile 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 Manage Data Sources page displays the current list of data sources. 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

   Show the status of the data source with respect to CA Performance Center. Often indicates a synchronization phase. For more information, see Synchronization (see page 18).

   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 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 18).

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.

New

Registers a new data source.

Edit

Lets you modify data source parameters.

Remove

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:

Managing Data Sources (see page 15)
Register a Data Source (see page 22)
Edit a Data Source (see page 24)
Synchronize a Data Source (see page 21)

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. Definitions created in CA Performance Center are sent to the data sources, but first, further changes to these definitions are prevented in the separate data source interfaces. The process of locking down data source administration is called "binding."

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 status 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. It 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

The Manage Data Sources page 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 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 currently under maintenance.

Disabled

Indicates that the administrator has disabled the data source.

More information:

View the Data Source Log (see page 22)
Data Source Synchronization Failed (see page 163)

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 17).

   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 records that are new since 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 performs the synchronization. A message appears only if any problems occur.

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 159).

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, check the Last Polled On date on the Manage Data Sources page.

Use the Data Source Log to investigate suspected errors with 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 17).

   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:

Synchronization (see page 18)
Synchronize a Data Source (see page 21)
Data Source Synchronization Failed (see page 163)

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 17).

   The Manage Data Sources page displays the current list of registered data sources.
3. Click New.

   The Data Source Administration dialog opens.
4. Select the type of data source 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. Enter the Host Name of the data source.

   The hostname is the IP address or DNS hostname of the server where the database for this data source is installed. For data sources in a distributed configuration, supply the hostname of the management console.
6. Type the port to use when contacting the data source. The port that you enter depends on the protocol you select.

   For more information, see the *CA Single Sign-On User Guide*.
7. 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*.
8. (*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.
9. Confirm whether the web console address is the same as the Host Name. If it is not, take the following steps:
   - Clear the 'Same as Data Source' check box.
   - Provide the web console hostname, port, and protocol.
10. Click Save to register the data source.

    CA Performance Center lists the data sources that you have registered in the Data Source List.

More information:

Test Data Source Connections (see page 24)
Edit a Data Source (see page 24)

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 162).

Edit a Data Source

You can edit registered data sources to change any of the parameters 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 17).

   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 22).
5. (Optional) Click Test to verify that the data source is connected properly.

   If the connection fails, see Data Source Test Failed (see page 162) for more information.
6. Click Save.

More information:

Register a Data Source (see page 22)
Test Data Source Connections (see page 24)

Remove a Data Source

You can remove a data source that you have registered to CA Performance Center. A data source that you remove can be registered to another CA Performance Center instance. The removal process also unlocks data source administration.

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Data Sources page (see page 17).

   The Manage Data Sources page displays the current list of registered data sources.
3. Select the data source that you want to remove (to unregister).
4. Click Remove, 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 already established in CA Performance Center are sent back out and shared among all registered data sources. Naming conflicts are resolved. And any changes 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 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 a List of SNMP Profiles

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.

   The page displays the current list of SNMP profiles.

   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.

   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.

   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.

Context Name

Specifies a collection of management information that is accessible by an SNMP entity. The Context Name is necessary for providing end-to-end identification and for retrieving data from an SNMPv3 agent. The Context Name is an octet string.

Authentication Password

Specifies the password for authentication using SNMPv3 and the selected authentication protocol.

Note: 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. In this case, SNMP data is missing for the affected interfaces: Interface and device names, interface speeds, and utilization data is missing from views.

Verify Authentication Password

Confirms the authentication password.

Privacy Protocol

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

Note: Specify None, DES, AES 128, or Triple DES as the Privacy Protocol. If AES 192 and AES 256 protocols are listed, do not select them. No SNMP data is returned for devices and interfaces that use the unsupported privacy protocols AES 192 and AES 256.

Use by Default

Indicates whether the information in this profile is used when not explicitly assigned to a device. If disabled (No), this profile is excluded from discovery in data sources that support the exclusion of profiles.

To perform any action on this page, select a profile, and then click a button.

More information:

Add an SNMP Profile (see page 28)

Add an SNMP Profile

Administrators can create SNMP profiles to let CA Performance Center 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.

   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 needed. 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.

   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

Specifies the authentication protocol to use when contacting devices associated with this profile. Select one of the following algorithms for authenticating SNMPv3 packets:

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

Authentication Password

Specifies the password for authentication using SNMPv3 and the selected authentication protocol.

Note: Some data sources do not support authentication passwords or privacy passwords that are shorter than eight characters. For example, CA Infrastructure Management Data Aggregator data sources enforce a minimum of eight characters. Consult the *Administrator Guide* for the data source and if applicable, provide passphrases greater than eight characters in length. 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-bit encryption)
- Triple DES
- AES 192 (192-bit encryption)
- AES 256 (256-bit encryption)

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

Privacy Password

Defines the password 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. You return to the Manage SNMP Profiles page. 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.

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.

   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 28).
5. Click OK.

   Your changes are saved.

   You return to the Manage SNMP Profiles page.

   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 70).
2. Navigate to the Manage SNMP Profiles page.

   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.

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 70).
2. Navigate to the Manage SNMP Profiles page.

   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 collected 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, host (see definition on page 168) 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:

Add an IP Domain (see page 36)
IP Domains (see page 32)
How IP Domains are Configured (see page 33)
Associating Items with IP Domains (see page 39)
Set Up Tenant IP Domains (see page 121)

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 113).
2. Create custom IP domains for each tenant. For more information, see Set Up Tenant IP Domains (see page 121).

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 21).

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 39).

   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 70).
2. Select Admin, User 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.

   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.

   DNS Proxy Address

   Is the IP address of the DNS proxy server.

   DNS Proxy Enabled

   Indicates whether the proxy address is enabled for this IP domain.

More information:

About IP Domains (see page 32)
How IP Domains are Configured (see page 33)
Add an IP Domain (see page 36)
Edit an IP Domain (see page 38)

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. It 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 70).
2. Navigate to the Manage IP Domains page (see page 35).

   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.

   Device Name Alias

   Indicates the aliases to use for managed devices. 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. The CSV file contains a comma-separated list of IP address-to-device alias mappings.

   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, retain the device IP address and delete the alias in the CSV file, and reimport the file.

For example:

```
172.24.36.107
```

To change an alias, modify the alias entry in the CSV file and reimport the file.

Description

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

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. (Optional) Select 'Enable DNS Proxy Address', and supply the IP address of the proxy server. This step is required if your network is located behind a DNS proxy server.
6. Click Save.

   The new IP domain appears in the list.
7. Repeat the steps as required to add more IP domains.

More information:

Device Name Display (see page 134)

More information:

About IP Domains (see page 32)
Add an IP Domain (see page 36)
Synchronize a Data Source (see page 21)

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 70).
2. Navigate to the Manage IP Domains page (see page 35).

   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 36).
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 70).
2. Navigate to the Manage IP Domains page (see page 35).

   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 33).

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 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, each Data Collector component can have only one IP domain assigned to it.

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 Data Aggregator components, see the *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 *Data Aggregator Administrator Guide*.

Change the Domain of Interfaces and CVIs

Administrators can change the parent domain for interfaces and custom virtual interfaces (CVIs), regardless of the domain of the parent router. Perform this step at any time after the Harvesters and routers are set up.

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. 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, which lists the current routers and their active interfaces.
2. Locate the interface or interfaces that you want to add to a 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, 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. Select the check box next to one or more interfaces or CVIs that you want to add to a domain.

   Note: By default, interfaces are associated with the domain of the parent router. You can put interfaces and CVIs in a different domain than the parent router, however.

4. Click Edit.

   The dialog for editing the interfaces or CVIs opens.

   Note: The Domain selection list is included in the editing dialog only if multiple domains exist.

5. Select the appropriate tenant/domain from the Domain list.

6. Click Save.

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

Note: You can also change the Harvester domain by editing Harvester details. If you change the Harvester domain, any routers and interfaces that are enabled after the change are assigned to the new domain automatically. The routers and interfaces that were enabled before the change continue to be associated with the previous Harvester domain.

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:

- Collector feeds.
- Client networks.
- 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 SLAs, and availability SLAs, 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 collector 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 Collection, 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 Collector Feed

You can instruct each Standard Collector 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 Collection, Collection Devices in the Show Me menu.

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

   The Collector Properties page opens.

4. Scroll down to the Collector Feeds list.
5. Click to edit a collector feed.
6. Select a custom IP domain.
7. Click Update.

   All items detected by this collector 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 Collection, 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 subnet, you cannot change its IP domain. If you add a server subnet to the wrong IP domain, you must delete the server subnet 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 Collection, Servers in the Show Me menu.

   The 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. Any items discovered previously do not receive retroactive associations.

Locations are not associated with custom IP domains if they contain any subnets. To begin associating Locations with a custom domain, follow the steps to select the domain for the Collector that monitors these Locations. Then you can manually edit Locations to remove subnets, select the custom domain, and then add the subnets back to them. Or you can follow the Location export procedure provided in the CA Unified Communications Monitor online Help.

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 threshold events coming from a data source to the Event Manager. 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.

A user only receives notifications for threshold events for an item in a group that the user has access to.

Consider the following information:

- Notifications are user-specific; users cannot see each other's notifications.
- 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 and product privilege can configure trap notifications.

Email

Sends email notifications to one or more recipients when an event is raised or cleared. Provides a link in the email to see 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 privilege 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 registered, enabled, and in a synchronized state of Available.

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:

EventManager Format Usage for Traps (see page 47)
nhLiveAlarm Format Usage for Traps (see page 49)

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/mibs

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/mibs

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 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.

Chapter 3: 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. In a well-planned deployment, roles let users access dashboards 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.

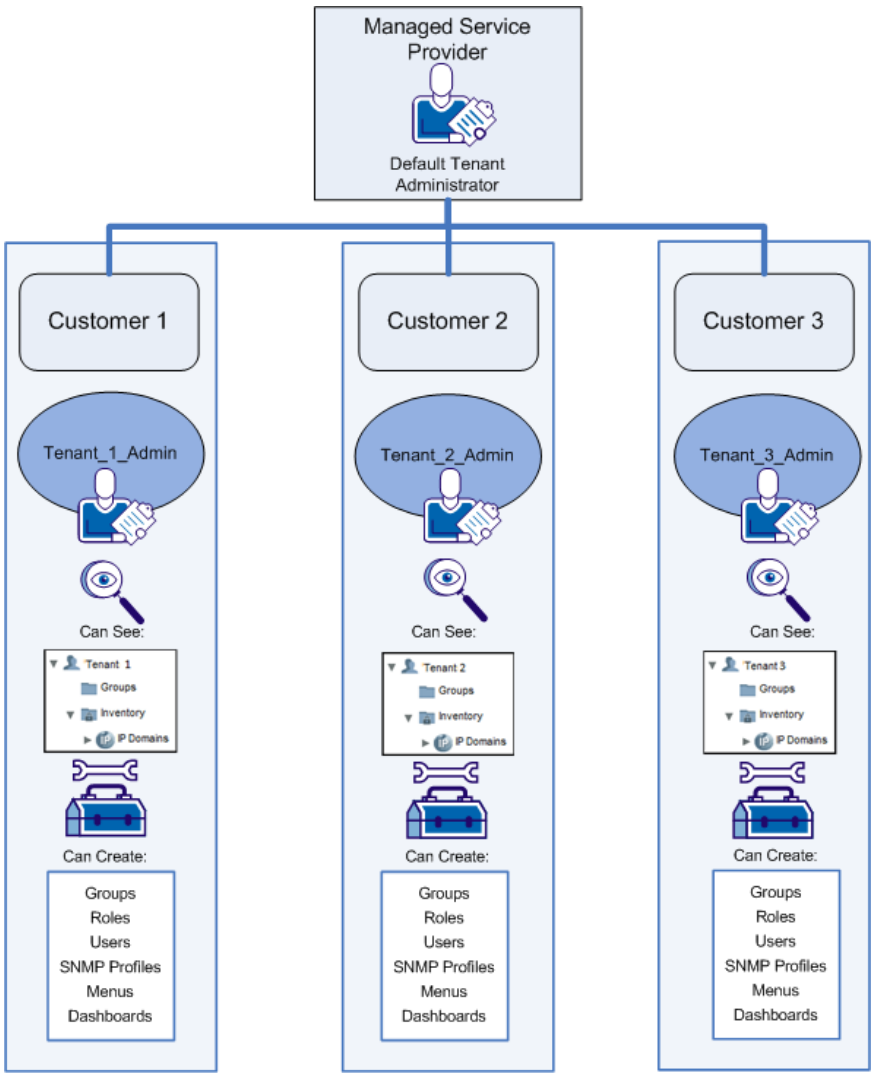
We recommend speaking with a CA technical representative to plan a strategy for creating a grouping and role structure. The best configuration meets your current requirements and is flexible enough to accommodate changes to your system.

Administrator Roles for Multi-Tenancy Support

When multi-tenancy is deployed, two distinct administrator roles are supported:

- Global Administrator (see definition on page 167) - 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 (see definition on page 170) - 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 116)
Administer a Tenant (see page 120)
Predefined Roles (see page 66)

How to Create a User Account

We recommend placing managed items in custom groups (see page 91) before creating user accounts. You assign custom groups to user accounts as "permission groups," which determine the data each user can view.

Create any custom roles (see definition on page 169) that you require before creating user accounts. Typically, however, the predefined roles (see page 66) are sufficient.

We recommend the following process for creating a user account:

1. Log in as a user with the required administrative role rights (see page 70).
2. Confirm that the appropriate groups exist, or create them if necessary.

   If data sources are already registered and data collection is occurring, system groups (see page 89) have been created automatically. Use these groups of items to build custom groups.
3. Confirm that the appropriate roles exist, or create them if necessary.
4. Add a user, and enter basic user information (see page 59).
5. Assign a role.
6. Assign permission groups (see definition on page 168).

   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 product privileges (see definition on page 168) to grant access to the data sources you have registered.
8. Test the user account by temporarily proxying (see page 64) it.

More information:

User Account Parameters (see page 53)
Edit a User Account (see page 62)
Clone an Existing User Account (see page 62)

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 70).
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:

   User 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:

Predefined User Accounts (see page 54)
Add a User Account (see page 59)
Roles (see page 65)
Role Rights (see page 70)

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 70).
2. Navigate to the Manage Users page (see page 58).

   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:

   User 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).

5. Click Permission Groups.

   The wizard advances to the next dialog.

6. Add permission groups to the user account, as follows:

   - Expand the groups in the Available Groups tree on the left so that subgroups appear.
   - Select a group or subgroup.
   - Click to add it to Selected Groups on the right.
   - Repeat as necessary.

   The selected permission groups appear in the Selected Groups pane.

   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.

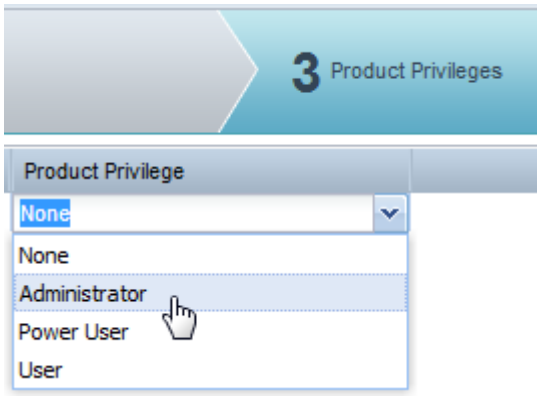
7. (Optional) Click the option to 'Enable My Custom Groups Functionality'.

   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 another group from the 'Default Group' drop-down list.

9. Click Product Privileges to advance the wizard to the next dialog.
10. Click the values shown in the Product Privileges column to enable drop-down lists.



Each registered data source has a separate list.

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 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.

11. Click Save.

The new user account appears on the Manage Users page.

More information:

Product Privilege (see page 81)
Permission Groups and User Accounts (see page 55)
How to Create a User Account (see page 57)
Clone a Tenant (see page 118)
Edit a User Account (see page 62)

Edit a User Account

You can modify a user account when the user's job responsibilities change, or when new permission groups are created. You must also edit user accounts to assign new roles to them. Any new roles you create are not used until you perform this step.

We recommend checking the permissions associated with each user account periodically to ensure that all items are being monitored. Each time a new data source is registered, new system groups are added to the Groups tree. In some cases, no CA Performance Center operators monitor these new groups until you explicitly add them to user accounts.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Users page (see page 58).

   The page displays the current list of user accounts.
3. Select the account that you want to change, and click Edit.

   Note: The rights and privileges assigned to the predefined administrator account, 'admin', cannot be modified. This user account must have administrator access to all registered data sources. If you select a group of accounts that includes the 'admin' account, you cannot modify any of the selected accounts.
4. Modify user account parameters as needed (see page 59).
5. Click Next to advance the wizard to the next dialog.

   Permission groups are shown in two tree structures.
6. Expand nodes in the Groups tree, and select the groups that this user must monitor.

   The groups appear in the 'Selected' tree to indicate that they are part of this user's permission set.
7. Select a new default group for this user.
8. Click Save.

   The changes are saved to the user account, and you return to the Manage Users page.

Clone an Existing User Account

You can create new user accounts quickly using the Clone feature. You can base new user accounts on an existing account, such as the predefined user account, "user".

Administrators can also create user account templates based on job function, which can be cloned to create individual accounts more easily. For security reasons, we recommend disabling the 'Enable user account' setting for templates so that CA Performance Center cannot be accessed unintentionally. Instead, enable CA Performance Center access as needed for the user accounts you create by cloning templates.

Follow these steps:

1. Log in as a user with administrative privileges.
2. Navigate to the Manage Users page (see page 58).

   The page displays the current list of user accounts.
3. Select a check box for the account you want to clone, and click Clone.

   The Clone User page opens. Most user account options are populated based on the cloned user account.
4. Enter a username for the cloned account.
5. Enter a password for the cloned account.
6. Click Save.

   The new account is saved.

More information:

Add a User Account (see page 59)
Edit a User Account (see page 62)
Predefined Roles (see page 66)
Predefined User Accounts (see page 54)

Delete a User Account

You can delete one or more user accounts at a time when they are no longer needed, for example, when an employee leaves the company.

Note: You cannot delete the two predefined user accounts (**admin** and **user**).

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Users page (see page 58).
3. Select the check boxes for the accounts you want to delete, and click Delete.
4. Click Yes to confirm the deletion.

   The accounts are deleted.

Proxy a User Account

Once you have created new user accounts, menus, or dashboards, you can test them. The Proxy feature lets you temporarily assume the identity of other CA Performance Center operators. You can proxy other users to validate significant changes or enhancements to dashboards. As a proxy, you see the same pages as the operator associated with the user account. You can also create dashboards that appear in another user's My Dashboards menu.

When proxying a user account, the tenant, permission groups, and user settings, including the time zone, are proxied. You can therefore test and verify these settings. Role rights and product privileges to data sources are not proxied. To proxy a user account from another tenant, you must first set the tenant scope (see page 120) to that tenant.

The proxied user account only persists within CA Performance Center. If you follow a drilldown path to a data source, the user account defaults to the original user account settings.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Users page (see page 58).

   The page displays the current list of user accounts.
3. Select the user account that you want to assume, and click Proxy.

   User account proxying begins. The 'Proxy User [User Name]' indicator appears in the upper-right corner of the page.

   Another login is not required.
4. Navigate the interface as desired to verify the dashboards, menus, and views for the user whose account is being proxied.
5. Stop proxying by clicking the X next to the Proxy User indicator.

   Or click '[change]' to start proxying a different user.

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. In a well-planned deployment, roles let users access dashboards that they require to perform their duties and restrict access to features that they do not require.

Roles are shared by CA Performance Center with registered data sources. When users follow a drilldown path to a data source, their role determines what they can see and do in the data source interface.

When you add a user to CA Performance Center, you select a role for the user account. You can create new roles or edit 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 quickly add new users 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 for which no corresponding role right exists. For example, only users with this role can create tenants, IP domains, SNMP profiles, and shared custom groups. **Note**: This role, the global administrator, cannot be modified.
Designer	All	■ Administer Shared Dashboards ■ Administer Menus ■ Administer Roles ■ Create a Dashboard ■ Edit Shared Views ■ Save Changes to Shared Views ■ Generate URLs from Views ■ Export to CSV ■ Send Reports by Email ■ Print a Dashboard ■ Edit Time Zone ■ Proxy Users ■ View Analysis Pages ■ View Conversations ■ View Hosts ■ View Inventory and Search ■ View Protocols ■ View ToS

Name of Role	Menus	Rights
IT Architect	All My Dashboards Infrastructure Health Capacity Planning Management Operations Displays	■ Administer Shared Dashboards ■ Create a Dashboard ■ Drill into Views ■ Drill into Data Sources ■ 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 ■ All rights to view data. See the Designer role for the full list.
IT Director	My Dashboards	■ Administer Shared Dashboards ■ Create a Dashboard ■ Drill into Views ■ Edit Time Zone ■ Export to CSV ■ 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 ■ Edit Shared Views ■ Save Changes to Shared Views ■ Generate URLs from Views ■ Export to CSV ■ Send Reports by Email ■ Send Reports on a Schedule ■ Print a Dashboard ■ Drill into Views ■ Drill into Data Sources ■ Edit Time Zone ■ All rights to view data. See the Designer role for the full list.
IT Operator	My Dashboards Operations Displays	■ 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 ■ 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.
VP of IT	My Dashboards	■ Create a Dashboard ■ Drill into Views ■ Edit Shared Views ■ Edit Time Zone ■ Export to CSV ■ Send Reports by Email ■ Print a Dashboard ■ Save Changes to Shared Views ■ 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. But you cannot modify the ‘Administrator’ role. We recommend changing the default passwords for better security.

More information:

Role Rights (see page 70)
View Current Roles (see page 76)
Proxy a User Account (see page 64)

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 each of 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.

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 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 Users

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

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 currently supported for CA Infrastructure Management Data Aggregator only.

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.

Role Rights for Dashboard and View Access

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

Browse to Device

Lets users navigate to the web page of a selected device.

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 view to see detailed data from a selected item.

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.

Set a Home Page

Lets users select a dashboard to set as the default page displayed when they log in.

View Analysis Pages

Lets users view and interact with the Analysis tab.

View Conversations

Lets users see specific client conversations.

View Hosts

Lets users see specific client host information.

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.

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

More information:

Data Source-Specific Role Rights (see page 73)
Predefined Roles (see page 66)
Add a Role (see page 77)

Data Source-Specific Role Rights

Each data source 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 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.

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 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
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 70).
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 assigned to it.

More information:

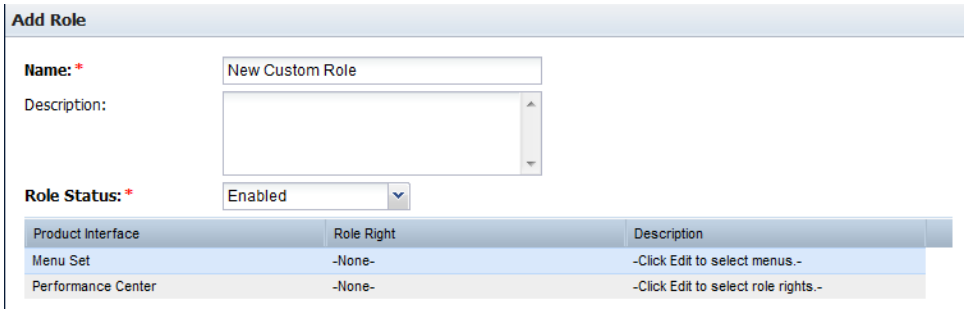
Edit a Role (see page 79)
Add a Role (see page 77)
Predefined Roles (see page 66)

Add a Role

If the predefined user roles (see page 66) 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 needs to be able to perform his or her 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 70).
2. Navigate to the Manage Roles page (see page 76).

   The page displays the current list of roles.

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 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 listed in the 'Available Rights' list can be added to the role. For more information, see Role Rights (see page 70).

10. Click an item on the left that you want to add to the role, and 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 70)
Data Source-Specific Role Rights (see page 73)
Edit a User Account (see page 62)

Edit a Role

The predefined user roles (see page 66) are useful for getting operators started using CA Performance Center. However, you can modify these roles, or you can create new ones to suit your unique environment and provide for the job 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 70).
2. Navigate to the Manage Roles page (see page 76).

   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, 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 77) 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 70).
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

Role Rights (see page 70)
Add a Role (see page 77)
View a List of Menus (see page 149)

Delete a Role

Once you have created a custom user role, you can delete it. To be deleted, 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 70).
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 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 70).

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 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. If you select a group of accounts that includes the admin account, you cannot edit 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 into 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 into the management console user interface, make sure 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 on the CA Network Flow Analysis data source to log into the NFA console. Product privileges also specify access to the Administration page and to certain functions:

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
- Interfaces page reports
- Existing reports on the Custom Reporting, Flow Forensics, and Analysis pages

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.

Power User

Gives User-level access and any additional abilities that are granted by the Role setting.

Administrator

Gives access to the Administration page and to all functions, including creating and managing user accounts, roles, groups, SNMP profiles, and scheduling for reports.

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 selected by an administrator. 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 and change them if desired.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Select Admin, User Settings, and click Users.

   The Manage Users page opens.

3. Select the user account that you want to edit.

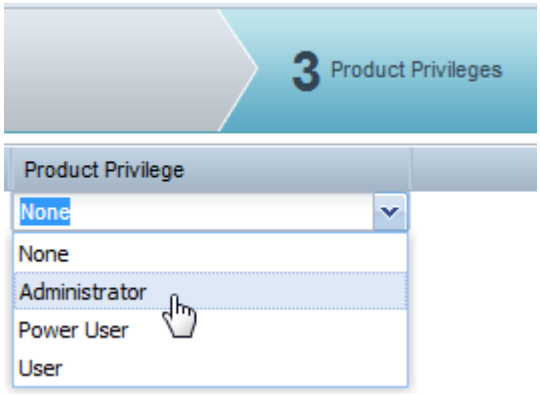
   Note: The rights and privileges assigned to the predefined administrator account, 'admin', cannot be modified. This user account must have administrator access to all registered data sources.

   The Create New User wizard opens.

4. Click Product Privileges to advance the wizard to the next dialog.

   All the data sources registered with CA Performance Center are listed on the Product Privileges page.

5. Click the values 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 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 Groups

This section contains the following topics:

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 they must 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:

Types of Groups (see page 88)
Custom Groups (see page 91)
Create a Custom Group (see page 99)
Groups for Multi-Tenant Deployments (see page 94)

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 shown in the Groups tree:

System Groups 

Are read-only groups automatically created by CA Performance Center based on information provided by 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 presented 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 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.

More information:

System Groups (see page 89)
Custom Groups (see page 91)
IP Domains (see page 32)
Use Groups to Customize Dashboards (see page 96)

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 assign them to user accounts as permission groups. Their read-only status is indicated by a lock icon:  .

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

Inventory 

Includes all managed items 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 collections of managed items. Collections are groupings of items that are monitored using the rules 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 94).

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, 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 the custom IP domains created by the administrator. Also includes the Default Domain, which contains all items not explicitly assigned to a custom domain. For more information, see IP Domains (see page 32).

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 each CA Performance Center operator permissions to access data.

The term *permission groups* describes groups that have been selected to act as high-level permissions. Assigned to user accounts, they precisely determine the items and data that each operator can view.

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. Or you can populate custom groups by adding specific items manually, such as routers or interfaces that are logically or geographically related.

You can add subgroups to permission groups to create narrower sets of accessible data. Using subgroups to allocate permissions helps users narrow their focus to investigate and monitor possible areas of concern. You can assign the subgroups to user accounts that need a narrow focus, and 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 need 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, they contain items and subgroups of items that are grouped by location. When you add site groups to the other custom groups in your tree structure, you can build reports that are organized both geographically and logically. Similar to other custom groups, site groups can contain subgroups. When building site groups, you can, for example, start with a region and add sub-groups containing cities. You can then add more subgroups to contain buildings within each city.

Grouping Best Practices

Creating custom groups to manage your or your customers' networks and devices 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 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 hierarchal 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. Additional 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 not explicitly associated with a tenant IP domain.

The groups that actually 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 additional 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 not explicitly assigned to a custom domain. For more information, see IP Domains (see page 32).

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. Click a tenant IP domain in the Groups tree to see the tenant's managed items.

Service Provider Defined Groups 

Includes groups that the global administrator has populated with shared items whose data this tenant should be able to 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 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 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 called *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 assigned to your user account determine the data 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 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 (see page 140).

Groups and Data Sources

The read-only system groups are specific to data sources. Most system groups are not created until 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 eHealth.

Use Groups to Customize Dashboards

When users log in to CA Performance Center, the dashboards 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 who has primary responsibility for Site A, but who functions as a backup for Site B, has permissions to 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. Add the views that all operators use on a daily basis to monitor your locations.

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

4. Edit each user account to select a new default group by following these steps:
   - Log in as a user with administrative privileges.
   - Navigate to the Manage Users page (see page 58).
   - Select the user account that you want to change, and click Edit.
   - Advance the wizard to the Permission Groups dialog.
   - Use the Default Group drop-down list to select the group whose data this user should see by default.
   - Click Save.
5. Repeat the previous steps to set a different default group for each user.

   When different users view the same custom dashboard, they see different data, 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 assigned to user accounts let operators effectively analyze data in a logical flow. They can drill down from data averaged from all managed items in a group into information about a single item from the same time frame.

The groups 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 88) in the left pane. Tabbed options in the right pane give access to group Items, Properties, and Rules (see page 101). Use the options on these tabs to populate and edit groups (see page 108).

More information:

Create a Custom Group (see page 99)
Add Managed Items to a Group Manually (see page 106)
Add Managed Items to a Group Using Rules (see page 101)
System Groups (see page 89)

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 make sure 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 88).

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—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. Or click My Settings, My Custom Groups.

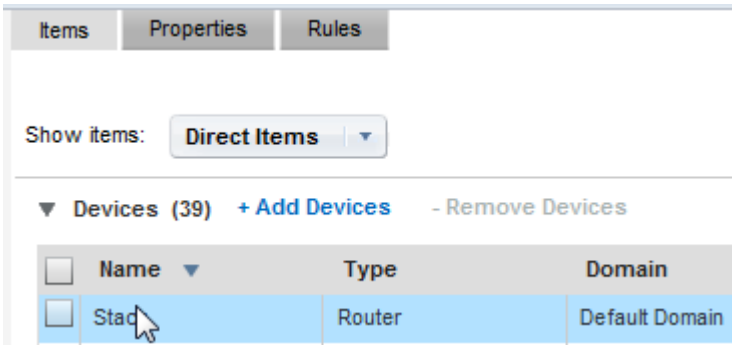
   A group management page opens.

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

   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 may be 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 you selected:

   Direct Items

   Includes 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 how the item was added, either 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. For example, when you enable inheritance for this group, all interfaces that are associated with a router are added to the group when the router is added.

   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:

Groups (see page 87)
Group Management (see page 97)
Types of Groups (see page 88)
Create a Custom Group (see page 99)

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.

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.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Groups page (see page 98).

   The page displays current groups in a tree structure.
3. Expand nodes in the Groups tree to find a location for the new group.
4. Right-click the node, and select Add New 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 or Site from the Group Type list.

   If you selected Site as the type, an additional parameter appears:

   Location

   Identifies a physical location that is associated with the site group, such as a city or a branch office.

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 91)
Permission Groups and Context Groups (see page 95)
Add Managed Items to a Group Manually (see page 106)
Add Managed Items to a Group Using Rules (see page 101)

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, if they do not meet rule requirements or are no longer monitored, items are removed.

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 that have rules applied to them.

Note: Group rules do not apply to domain groups.

Follow these steps:

1. Navigate to the Manage Groups page (see page 98).

   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.

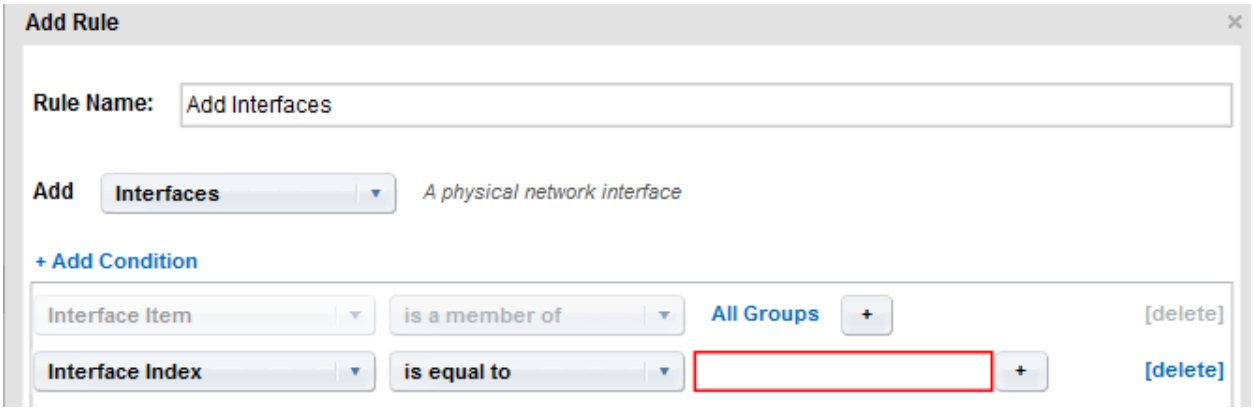
7. Supply a name for the rule in the Rule Name field.

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 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, and IP address.

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

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

    Important! 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 a text string to match in the remaining condition field. For example, to add all routers and servers in the Southwest region, supply a string 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' drop-down list appears.

14. (Optional) To add 'AND' matches, click Add Condition.

    Three more dropdown 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 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 add managed items automatically to custom groups as items are discovered during monitoring. Once you have created rules, you can edit them. 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 70).
2. Navigate to the Manage Groups page (see page 98).

   The page displays current groups 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 as links.
7. Click the [edit] link.

   The Edit Rule window appears.
8. Make the desired changes to existing filters, add filters or subrules, or remove filters or subrules as needed.

   A [delete] link appears next to each filter so that you can delete it.
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 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 70).
2. Navigate to the Manage Groups page (see page 98).

   The page displays current groups in a tree structure.
3. Select the group with the rule that you want to modify by adding a subrule.
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 you have created to add managed items to a group automatically. When you delete a group rule, any items added to the group where that rule was applied are removed immediately. The items themselves 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 70).
2. Navigate to the Manage Groups page (see page 98).

   The page displays 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. Use the mouse to hover over the rule.

   Options to [edit] or [delete] the rule appear as links.
6. Click the [delete] link.

   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 that you select. Adding managed items to groups individually can be necessary when you are fine-tuning group structure. However, setting up group rules is usually a more effective strategy.

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.

Follow these steps:

1. Navigate to the Manage Groups page (see page 98).

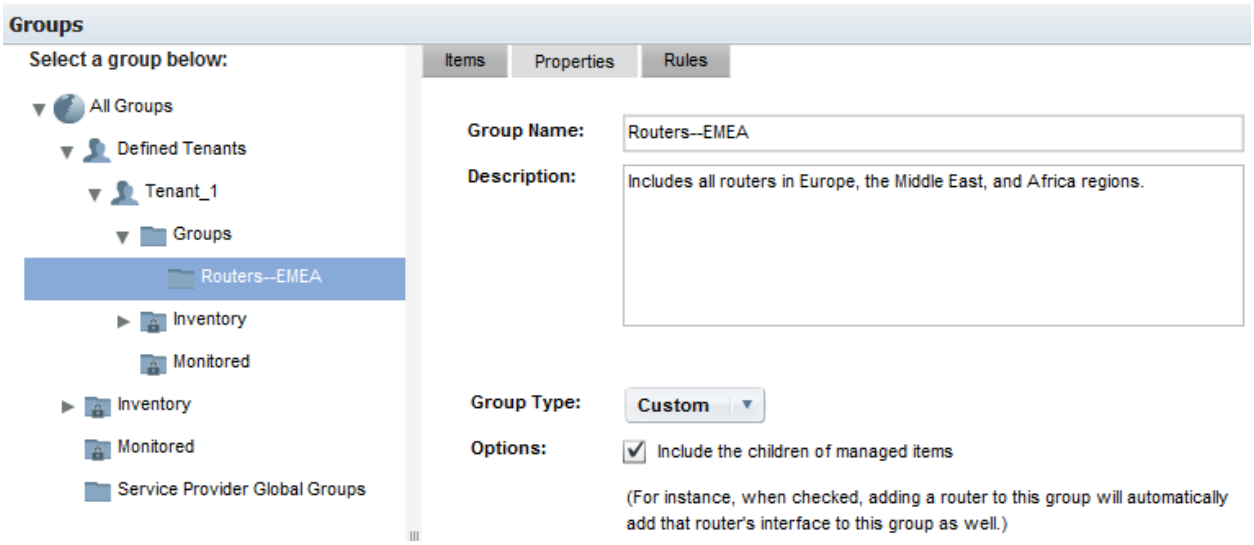
   The page displays current groups in a tree structure.
2. Expand nodes in the Groups tree to locate and select the group to which you want to add managed items.

   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 Items tab.

   The Show Items list appears. It does not apply to groups that do not yet 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 registered, and the items discovered.

   To see additional pages of items, click the links below the list. Or use the Search field to search for an item in the list.

9. Select items by clicking their check boxes. Click the check box in the table header row to select all items on a page.

10. Click Add Items.

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

11. 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 additional 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 its group references. Removing a group also deletes all of its references.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Groups page (see page 98).

   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.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Groups page (see page 98).

   The page displays current groups 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 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.

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. Any groups that the deleted group contains–its subgroups–are also deleted.

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

Follow a slightly different procedure to Delete a Group Reference (see page 110). A group reference is a copy of another group. Its icon indicates that it is a copy: 

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Groups page (see page 98).

   The page displays current groups in a tree structure.

3. Select the group that you want to delete where it appears in 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, and select Remove Group.
5. Click Yes to confirm the deletion.

   The selected group and all of its subgroups are deleted.

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 additional tab in the right pane. Use the "Remove References" tab to see and remove references to that group.

If you delete a group that has been referenced somewhere, all its references are also deleted. By contrast, if you delete a group reference, the original group is not affected.

Deleting a subgroup that is a reference affects neither the original group, nor the group that contains it. But to delete a group that contains subgroup references, delete all the references before deleting the group. Otherwise, issues arise when you attempt to remove the references.

For example, if several offices have consolidated to a single location, delete all references to the closed offices so that they no longer come up in search results. Deleting one reference does not delete them all.

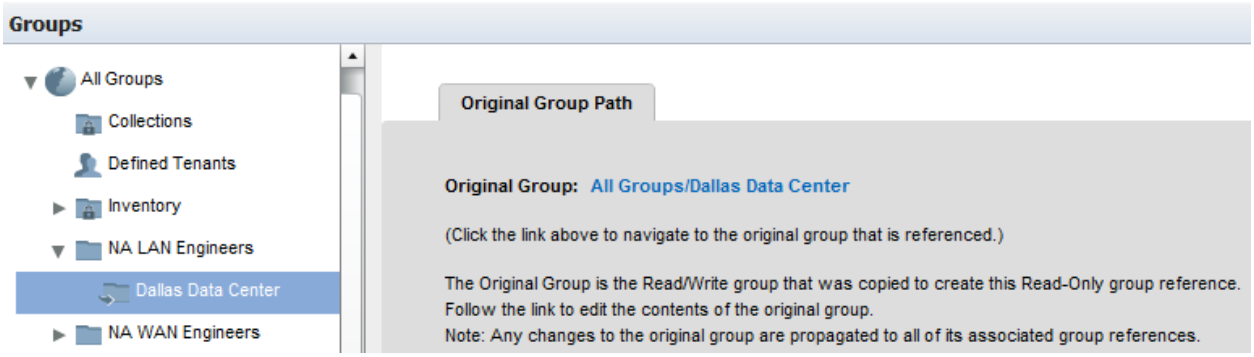
Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Groups page (see page 98).

   The page displays current groups 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. Their path in the Groups tree is included.
7. Select the group reference that you want to delete.
8. Click Remove Group Reference.
9. Click Ok to confirm the deletion.

   The selected group reference is deleted.

Chapter 6: Creating and Managing Tenants

This section contains the following topics:

About Tenants

Adding 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. You can associate monitored devices and product settings for each customer with the tenant definition in separate steps. Each tenant must contain at least one IP domain. You and 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 and system groups
- Custom dashboards
- Custom menus

Custom IP domains (see page 32) 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.

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 87) 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 113).

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:

About Tenants (see page 113)
Add a Tenant (see page 116)
Administer a Tenant (see page 120)
Set Tenant Scope (see page 120)

Add a Tenant

Only a user with the predefined Administrator role can add tenant definitions to distinguish among customer networks and systems. This user (a "global" administrator) is equivalent to the 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 (see definition on page 170) 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 118) feature.

Follow these steps:

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

   Note: A tenant administrator cannot create tenants.

2. Navigate to the Manage Tenants page (see page 115).

   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 default administrator for this tenant. Enter information for the following parameters:

   Administrator

   Is a login name for the 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 default tenant user. 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 120).

More information:

Administrator Roles for Multi-Tenancy Support (see page 55)
Clone a Tenant (see page 118)

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 120).

Follow these steps:

1. Log in as a user with the Administrator role.
2. Navigate to the Manage Tenants page (see page 115).

   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 116) 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 115).

   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 119).

Setting Up Tenants

The topic Add a Tenant (see page 116) 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:

Administrator Roles for Multi-Tenancy Support (see page 55)
Add a Tenant (see page 116)
Set Tenant Scope (see page 120)
Administer a Tenant (see page 120)

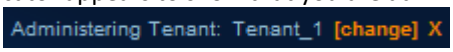
Set Tenant Scope

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 115).

   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 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.
5. (Optional) Change the tenant scope to another tenant by clicking the [change] link next to the 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.

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.

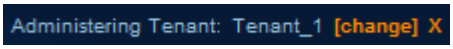
When the tenant scope has been set, the procedures for administering a tenant are identical to the procedures to perform in a single-tenant environment.

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 120) 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 Groups (see page 123)
Set Up Tenant IP Domains (see page 121)
Set Up Tenant Menus (see page 129)
Set Up Tenant Roles (see page 124)
Set Up Tenant SNMP Profiles (see page 122)
Set Up Tenant Users (see page 127)

Set Up Tenant IP Domains

Tenant definitions are created and configured as separate steps. A tenant definition must contain at least one IP domain, a range of IP addresses that correspond to the managed items in the tenant environment.

When 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 120) 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, User 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 36).

5. (Optional) Select 'Enable DNS Proxy Address', and supply the IP address of the proxy server. This step is required if your network is located behind a DNS proxy server.

6. 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 120) 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 28) 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.

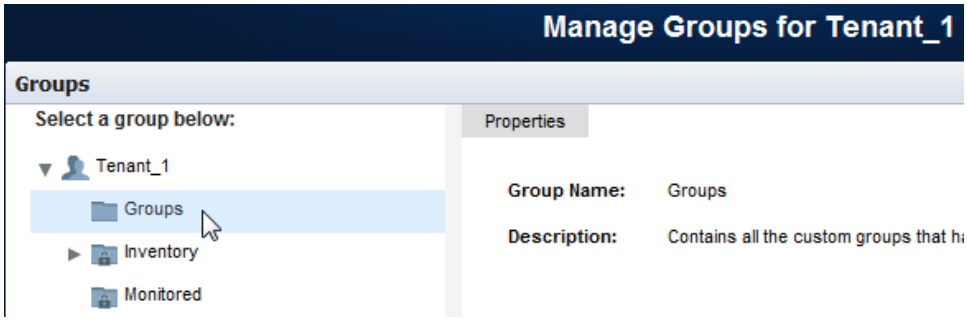
   Or set the tenant scope (see page 120) to access tenant configuration while logged in as a global administrator.

   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 89) 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 106) by adding items in the Manage Groups interface.
   - Create rules (see page 101) 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 55).

Follow these steps:

1. Log in as a tenant administrator associated with this tenant.

   Or set the tenant scope (see page 120) 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.

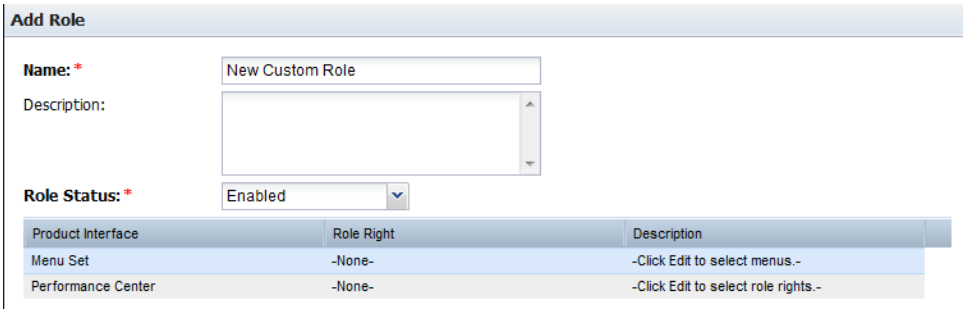
   Description

   (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:

Role Rights (see page 70)
User Account Parameters (see page 53)
Add a Role (see page 77)
Add a User Account (see page 59)

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 120) 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:

   User 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 120) to access tenant configuration as a global administrator, and then proxy a tenant administrator (see page 64) 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 115).

   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: Working with Dashboards

This section contains the following topics:

Viewing Data in CA Performance Center

Dashboard pages display 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 (see page 138) dashboards. They can, for example, place views of application performance data beside views of volume data to help troubleshoot issues from a single page.

The predefined (factory) dashboards are organized into workflows. You can drill down from Top N views to more detailed metrics from a narrow context, such as an individual device. Workflows let you see data that may be 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.

Administrators can 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 at the summary, device, or item level.

Views showing data for a group are CA Performance Center-generated views that contain rollups of data from data sources. Views showing data for a server or device, or detailed metrics from a narrow context, often provide a drilldown path directly to the data source. The Single Sign-On (see definition on page 169) feature lets you seamlessly navigate from a dashboard to a data source interface.

More information:

Product Privilege (see page 81)

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 (see page 133) for the data shown in the view.

  Note: Users with the 'Save Changes to Shared Views' role right (see page 70) 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.

More information:

Performing Searches (see page 134)
Role Rights (see page 70)

Change the Data Context for a View

You can change the context for a single view on a dashboard. The context for a view or page is driven by filters that are appropriate for each type of view. Change the context to show data from a different managed item or from a different set of managed items.

Changing the context for a view is useful for troubleshooting performance issues. For example, assume that a view does not show performance data that appears to correlate with a problem you are investigating. You can select another managed item to compare data from the same time frame. You can edit a view of disk utilization for physical servers to show disk utilization for Virtual Machines instead. Or you can compare data from different geographical regions by leveraging your group structure to change the group context.

Follow these steps:

1. Open the dashboard that contains the view that you want to modify.
2. (Optional) Change the time frame, if necessary.
3. Click the Edit icon  in the view whose context you want to change, and select Edit from the menu.

   The View Settings dialog opens.
4. Change the view Title or Subtitle to reflect the new context.

   The context types that are available depend on the type of view.
5. Take one of the following steps, depending on the context type you selected:
   - Click to expand folders in the Groups filter tree, and select the group whose data you want to see in the view.
   - Locate the managed item whose data you want to see in the view, and click the link in the table.

6. Select the scope of your changes from the Apply Changes drop-down. Select one of the following options:
   - For All Tenant Users: Saves the changes so that they are only available to users associated with your tenant (possibly the Default Tenant).
   - My User Account: Saves the changes to your user account as a default for this view.
   - My Current Session: Reverts the changes when you log out.

   Note: The availability of these options depends on your user account role rights.
7. Click Save.

   The view is updated with data from the new context.

You can also change the context for a dashboard (see page 140), which applies the selected group or managed item as a filter to all views on the page.

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.

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.

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 136).

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 136).

   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.

Custom Dashboards

Custom dashboards are useful for displaying data from a particular item or group of items. With a custom dashboard, you can select the item context for individual views and can make other modifications to meet the requirements of a selected operator.

Custom dashboards are often used on a temporary basis to troubleshoot an issue. However, they are also deployed on a long-term basis to monitor categories of items. For example, an operator who is responsible for a region requires a dashboard that shows only items in that region. Or an operator might require a dashboard to monitor all ESX servers.

To create a custom dashboard quickly, you can edit an existing dashboard and save it with a new title. Your user account must have the Edit Dashboards role right.

Create a Custom Dashboard

Users with the necessary role right can create a custom dashboard. They can select views for the dashboard and their location on the page. They can also select the menus in which it appears so that the dashboard can be shared with other CA Performance Center operators.

The views in a custom dashboard can also be customized. For example, you can select a group context, or you can specify a custom view title.

You can customize the predefined CA Performance Center dashboard pages, or you can add new dashboards. You can select the views and data context for custom dashboards.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Click the Dashboards tab.

   The Available Dashboards page opens. Each view on the page corresponds to a menu.
3. Click Add Dashboard next to the menu where you want the new dashboard to appear.

   The Add Dashboard page opens.
4. Complete the following fields:

   Dashboard Menu

   Is the menu where you want the dashboard to appear.

   Menu Item

   Is the name of the dashboard as you want it to appear in the menu.

   Dashboard Title

   Is the name that you want to appear at the top of the new dashboard.
5. (Optional) Select a layout template for the dashboard.

   Each layout treats the page as a table with rows and columns for views. The Layout buttons indicate the number of views in each column and row on the page.

   Note: We recommend selecting a layout before adding views.
6. Expand the categories of views shown in the left pane.
7. Select a view that you want to add to the page from one of the expanded lists.

   Note: The maximum number of views per dashboard is 25.
8. Click and drag the view to the page layout, and drop it where you want it to appear.

Note: By default, the context is Summary. With the *Summary context* setting, the available views display summary data for the current group context of the dashboard. The Summary setting does not require you to select a specific group or item. Summary views dynamically update the context when you change the context of the page.

9. (Optional) Apply a group or context filter to the views. Views with a selected context always display data for that context; they do not inherit the context of the dashboard. For example, if you set the context filter to Group A and add a view to the dashboard, that view will always display data for Group A, even after you change the dashboard context to Group B.

   You can select a group, device, or interface context by taking the following steps:

   a. Click Filter by: Summary.

   b. Select a Context Type, such as a type of managed item. Select Group to see the Groups tree.

      By default, the Context Type list is filtered to show only items and item types to which you have access. For example, if you are not monitoring any servers, the Context Type list does not include the Servers option. Select 'Show All Context Types' to see all context options.

   c. Select a specific context item or a group context.

   d. Click OK to save the new context filter.

10. (Optional) Click Clear Filter on the main Edit Dashboard Layout page to revert to the Summary filter.

11. Click Save to save the dashboard and add it to the selected menu.

    To discard the changes you made, click Clear.

Edit a Dashboard

You can customize dashboard pages if your user account has the 'Administer Shared Dashboards' or the 'Create a Dashboard' role right. You can add or remove data views, rearrange views, or select a different context filter for a dashboard. You can then export the new dashboard as a report.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Use the Dashboards tab to access the dashboard that you want to edit.
3. Click the More menu, and select Edit Dashboard.

   The Edit Dashboard Layout page opens.

4. Change the following menu and dashboard options, as needed:

   Menu for Dashboard

   Is the menu where you want the dashboard to appear. The default is the menu that you used to open this dashboard page.

   Menu Item

   Is the name of the dashboard as you want it to appear in the menu.

   Dashboard Title

   Is the name that you want to appear at the top of the new dashboard.

5. Select a layout template for the dashboard from the Layout buttons.
6. Remove unwanted views from the dashboard 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.

   Note: By default, the context is Summary. With the *Summary context* setting, the available views display summary data for the current group context of the dashboard. The Summary setting does not require you to select a specific group or item. Summary views dynamically update the context when you change the context of the page.

7. (Optional) Apply a group or context filter to the views. You can select a group, device, or interface by taking the following steps:

   a. Click Filter by: Summary.

   b. Select a Context Type, such as a type of managed item. Select Group to see the Groups tree.

      By default, the Context Type list is filtered to show only items and item types to which you have access. For example, if you are not monitoring any servers, the Context Type list does not include the Servers option. Select 'Show All Context Types' to see all context options.

   c. Select a specific context item or a group context.

   d. Click OK to save the new context filter.

   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.

8. Click to expand the categories of views.
9. Select a view, drag it to the Layout pane, and drop it where you want it to appear.

   Note: The maximum number of views per dashboard is 25.

10. Click Save.

    The dashboard page refreshes to reflect your changes.

Change the Context for a Dashboard

You can customize a dashboard by selecting a different data context for the data. The default group setting for the views that are shown on all dashboards is 'All Groups'. When you select another group for a standard dashboard, you apply a new filter to all views on the page. From a context page, such as details about a single router, you can select another managed item as the view context.

You can also view dashboards in multiple windows and apply a different data context to each dashboard.

Follow these steps:

1. Navigate to the dashboard that you want to modify.
2. (Optional) Change the time frame, if necessary.
3. Click the [change] link above the time period selectors.

   [change] link

   Lets you select another group or managed item context for reporting.

   A dialog opens with filtering options.
4. Click to select another managed item. Or expand nodes in the Groups tree to select a group context.

   Data from the new item or group will be shown in the view.
5. Click OK.

   A message indicates that the change has been saved.

   All views on the page are refreshed to reflect the new data context.
6. (Optional) Open another browser instance, log in, and open the same dashboard.

   You can now compare the same views with two different item context settings.

More information:

Permission Groups and Context Groups (see page 95)
Change the Data Context for a View (see page 133)

Change the Time Frame for a Dashboard

You can change the time frame for a dashboard you are viewing. Change the time frame to see performance data from an earlier time of day or from another date.

Changing the time frame is useful for troubleshooting performance issues. For example, if data from the past day contains an anomaly, you can change the time frame to show data from the last seven days. The time frame helps you determine whether the same issue is occurring regularly.

When you change the time frame for a dashboard, it is applied to all views on the page, and to all dashboards in that window. However, you can view dashboards in multiple windows and can apply a different time frame to each dashboard.

Follow these steps:

1. Select a dashboard from the Dashboards tab.
2. Click to select some of the following time and date options on the toolbar:

   Time period drop-down list

   Lets you select a predefined time frame for the data.

   Default: Last Hour.

   Back button

   Shifts the time frame for the data back by one increment of the present interval (such as Last Day or Last Hour).

   Date and Calendar drop-down lists

   Let you select a start and end date for the data from a calendar view.

   Time of Day drop-down lists

   Let you select a start and end time from a list of 15-minute time intervals in the 24-hour format.

   Forward button

   Shifts the time frame for the data forward by one increment of the present interval (such as Last Day or Last Hour).

3. To define a custom time frame, take one or more of the following steps:
   - Click the start date and select a new start date from the calendar that appears.
   - Click the end date and select a new end date from the calendar that appears.
   - Click the start hour or minute and select a new hour or minute from the drop-down menu.
   - Click the end hour or minute and select a new hour or minute from the drop-down menu.

4. Click Set.

   The page is refreshed, and the data displayed in the views reflects the new time frame.

5. (Optional) Scroll backward or forward in time. Use the Back and Forward buttons on either side of the timestamp to shift the time frame by one increment of the present interval.

   If you are viewing data for the last day, click the left arrow to scroll back in time by one day. Or click Latest to see the most recently collected data.

Sharing Data with Other Users

Multiple options let you share dashboards and views with coworkers. You can export a dashboard to a static report in PDF format. You can print reports or send them by email. You can set up a schedule to send a report automatically on a regular basis.

You can also export individual views. You can publish views on a web page, such as an intranet site. Or you can export data from a view to a file in CSV format. For all data-export options, certain user account role rights are required.

Print a Report

If your user account has the required role right, you can export the current dashboard contents as a printed report. The Print feature first displays the current dashboard page in PDF format.

Follow these steps:

1. Navigate to the dashboard that you want to export as a report.
2. (Optional) Change the time frame (see page 141).
3. Click the Print link on the toolbar.

   The report is exported as a PDF. Typically, it is displayed in a separate browser window.

   The data uses the current dashboard settings.

4. (Optional) Save the PDF to the local computer using the options in your PDF viewer.
5. Click the Print icon in the browser toolbar.

   The report page is sent to the local default printer.

Send a Report by Email

You can export the current dashboard contents as a report attached to an email message. The Email feature lets you specify the email address of the recipient and also the Subject line of the email message. The report is attached to the message as a document in PDF format.

Sending reports as email attachments requires an administrator to specify an SMTP server. Your user account must also have a role with the 'Send Reports by Email' role right. For more information, see the Related Topics.

Follow these steps:

1. Open the dashboard that you want to send in an email message.
2. (Optional) Change the time frame, if necessary.
3. Click the Email icon on the toolbar.
4. Supply information for the following fields:

   Send To

   Specifies the email addresses where the report should be sent. Use the standard format:

   <name>@<domain>

   Note: Use commas or semicolons to separate multiple addresses. Or you can enter an email alias that includes multiple recipients.

   Subject

   Appears in the email Subject line; describes the emailed report.

   Example: The dashboard title and any components whose data is included in the report.

   Message

   (Optional) Is a message to accompany the emailed report.
5. Select Send Now to send the email message immediately.

   Or select Send on a Schedule to create a schedule to send the email message on a regular basis. For more information, see Set Up a Recurring Email Schedule (see page 144).
6. Click OK.

   The CA Performance Center server generates a PDF from the current dashboard and sends the report as an attachment to an email message.

More information:

Set the Email Server (see page 12)
Role Rights (see page 70)
Set Up a Recurring Email Schedule (see page 144)

Set Up a Recurring Email Schedule

Each dashboard contains options to export and send data in reports. Your user account must have the 'Send Reports by Email' role right.

You can send a report by email immediately, or you can create a schedule for recurring emailed reports. For example, you can email interface utilization reports each week to coworkers in the IT department for capacity planning.

Note: The administrator must specify an email server to enable this feature.

Follow these steps:

1. Log in to CA Performance Center and select a report from the menus on the Dashboards tab.
2. Click Email.

   The Email Dashboard dialog opens.
3. Supply information in the following fields:

   Send To

   Specifies the email addresses where the report should be sent. Use the standard format:

   <name>@<domain>

   Note: Use commas or semicolons to separate multiple addresses. Or you can enter an email alias that includes multiple recipients.

   Subject

   Appears in the email Subject line; describes the emailed report.

   Example: The dashboard title and any components whose data is included in the report.

   Message

   (Optional) Is a message to accompany the emailed report.
4. Select one of the following Scheduling Options:

   Send Now

   Sends the email message immediately.

Send Daily

Sends the email message once per day. If enabled, reveals check boxes where you can select the day of the week when the report is sent.

Default: Send the emailed report every weekday (Monday - Friday) at 0:30 hours in the time zone of the logged-in user. The data in the report reflects the previous 24 hours.

Send Weekly

Sends the email message once per week. If enabled, lets you select the day of the week to send the report.

By default, the weekly schedule sends the emailed report every Sunday at 01:00 in your time zone.

Default: The data in the report reflects the previous seven days (Saturday - Sunday).

Week Ends on

Determines the day when the week ends. The start of the week is automatically adjusted to include seven days.

Send Monthly

Sends the email message once per month. Sends the report on the first Sunday of each month at 01:00 in the time zone of the Management Console. The data in the report reflects the previous 30 days.

Send Email at

Determines the time of day when the message is sent. The start of the month is automatically adjusted to include 30 days.

Send Quarterly

Sends the email message once per quarter. Sends the report on the first Sunday of each quarter at 01:00 in the time zone of the Management Console. The data in the report reflects the previous three months.

First Quarter Ends in

Determines the month when the quarter ends. The start of the quarter is automatically adjusted to include three months. All other quarters are also adjusted to proceed from the first quarter.

Send Yearly

Sends the email message once per calendar year. Sends the report on the last day of the month you select for the 'Year ends in' parameter. The data in the report reflects the previous 12 months.

Year Ends in

Determines the month when the year ends. The start of the year is automatically adjusted to include 365 days.

Send email at [time of day]

Sends the email message at a time you select.

5. Click Save to save the schedule.

   The report is saved as a PDF file and attached to an email message. The message is sent immediately or according to the schedule you selected.

Manage Email Schedules

Users with the required role rights can set up schedules to send reports by email on a recurring basis. Selected dashboard data is exported in report format and sent to designated users according to a regular schedule.

Users who lack administrative role rights can edit the email schedules that they have created themselves. But if your user account has the required administrative role rights, you can also edit or delete the schedules that other users have created.

Follow these steps:

1. Log in as a user with administrative role rights (see page 70).
2. Select Admin, User Settings, and click Scheduled Emails.

   The Manage Scheduled Emails page opens.

   The page displays the current list of email schedules.

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

3. Select the email schedule that you want to change, and click Edit.

   The Email Dashboard dialog opens.

4. View or change the settings for email schedules. For more information, see Set Up a Recurring Email Schedule (see page 144).
5. Click Save.

Generate a URL for a View

You can export a view and share it with coworkers who do not have access to dashboards. CA Performance Center can generate a special uniform resource locator (URL) to recreate a selected data view on demand. The URL lets you add the view to a web page or intranet site to share performance data with coworkers. The Generate URL feature lets you involve others in capacity-planning and infrastructure upgrade decisions and lets you share status information.

Follow these steps:

1. Log in as a user with the 'Generate URLs from Views' role right.
2. Navigate to the dashboard that contains the view for which you want to generate a URL.
3. Click the Edit icon  on the view, and select Generate URL.

   The Generate URL dialog opens. The URL is displayed in the URL field.
4. Enable or disable the following required parameters for the exported view:

   View Container

   Displays the chart or graph with a surrounding container. The container includes the title of the view in a title bar and a black outline around the chart or graph.

   Default: Enabled

   Drill Down

   Enables users to drill down from the view into the underlying data source for more detailed data. These users must have a minimal product privilege to the data source and the 'Drill into Data Sources' role right to use this feature.

   Default: Enabled.
5. Select from the following time frame options:

   Time Options

   Let you change the time frame for the data in the exported view. Supply a custom time frame in the Start Time and End Time fields, or select a Time Range from the drop-down list.

Token Expiration Options

Control view expiration. The default, 'Never' expires, lets the exported view display indefinitely.

If you want the view to expire, select a timeout period from the Token Expiration drop-down list. The URL includes an encrypted token that causes the view to expire after the specified timeout period.

6. (Optional) Click Preview to see how the view looks with the options you have selected.
7. Copy the URL displayed at the top of the page to the Clipboard.
8. Paste it to the destination where you want to display the view.
9. Click OK.
10. The Generate URL window closes.

Export a View to a CSV File

You can export the contents of a view to a file in comma-separated values (CSV) format. The .csv file format is compatible with spreadsheet applications, such as Microsoft Excel. When you export a view, all view contents are exported as raw data.

Note: A limit of 5000 managed items is enforced for CSV export. Items that exceed the limit are not exported from the database.

Follow these steps:

1. Log in as a user with the 'Export to CSV' role right.
2. Navigate to the report that contains the view that you want to export.
3. Click the Edit icon  on the view, and select Export to CSV.

   The browser prompts you with options to open or save the exported file.
4. Select the Save option if you want to supply a filename.
5. Browse to the location where you want to save the file, and click Save.

   The view is saved as a file in .csv format.

Organizing Dashboards in Menus

Dashboards are organized into menus that describe a troubleshooting or monitoring purpose. You see a list of available dashboards and menus when you hover on the Dashboards tab.

Users with the required administrative role rights (see page 70) can reorganize menus. They can also create custom menus that contain predefined or custom dashboards. They can then associate the new menus with user account roles. When product operators log in, the dashboards they require to perform their daily tasks are organized in a meaningful way.

Administrators can remove a dashboard from any menu and add it to a shared menu or to the My Dashboards menu of selected user accounts.

View a List of Menus

The Manage Menus page contains a list of currently defined menus. Before you add custom menus, only predefined menus are included in the list. The user account role determines the menus that each user can access.

Custom menus are defined for each tenant. Only the factory menus are shared among tenants. The global administrator sees a list of menus not explicitly associated with a tenant.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Select Admin, User Settings, and click Menus.

   The Manage Menus page opens.

   The page displays the current list of menus. The following menus are provided with CA Performance Center and appear by default in the Menu List:

   Infrastructure Health

   Contains summary and overview dashboards with at-a-glance views of system and device health and performance, events, and threshold compliance.

   Application Health

   Contains overviews and detailed analysis of application performance. Also contains related dashboards, such as performance by protocol and server performance.

   Capacity Planning

   Contains dashboards that are related to projections, thresholds, and recent changes to systems or devices.

Management

Contains at-a-glance scorecards and overview dashboards, as well as high-level summary and comparison dashboards.

Operations Displays

Contains high-level overview dashboards appropriate for display in the Operations Center and for use by Network Operators.

To perform any action on this page, select a menu, and then click a button.

If any dashboards have been customized, the following additional menu appears:

My Dashboards

Contains frequently used dashboards for an individual user account. Any dashboards that this user modified become available in this menu.

Note: Users with the required role right can edit the My Dashboards menu for a user account by proxying that user account. For more information, see Proxy a User Account (see page 64).

More information:

Custom Menus (see page 150)
Add a Menu (see page 151)
Edit a Role (see page 79)

Custom Menus

Administrators and designers can create custom menus for the Dashboards tab. Custom menus let you determine the dashboards available to each user account. Ideally, at login, CA Performance Center operators see three or four menus on the Dashboards tab that contain only the data that they require.

If your user account has the necessary role right, you can also create custom dashboards (see page 137) to populate a custom menu.

Custom dashboards that are included in a user's My Dashboards menu are not visible to other users. Users can therefore copy a dashboard from a factory menu to their My Dashboards menu and then customize it.

A custom menu is not available to any users until the administrator edits a role to include it. The role must, in turn, be assigned to a user account.

Add a Menu

Custom menus let you organize dashboards and make them available to selected roles. Administrators and designers can create custom menus and can select dashboards for each menu.

A custom menu is not available to any users until the administrator edits a role to include it. The role must, in turn, be assigned to a user account.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Menus page (see page 149).

   The Manage Menus page displays the current list of menus.
3. Click New.

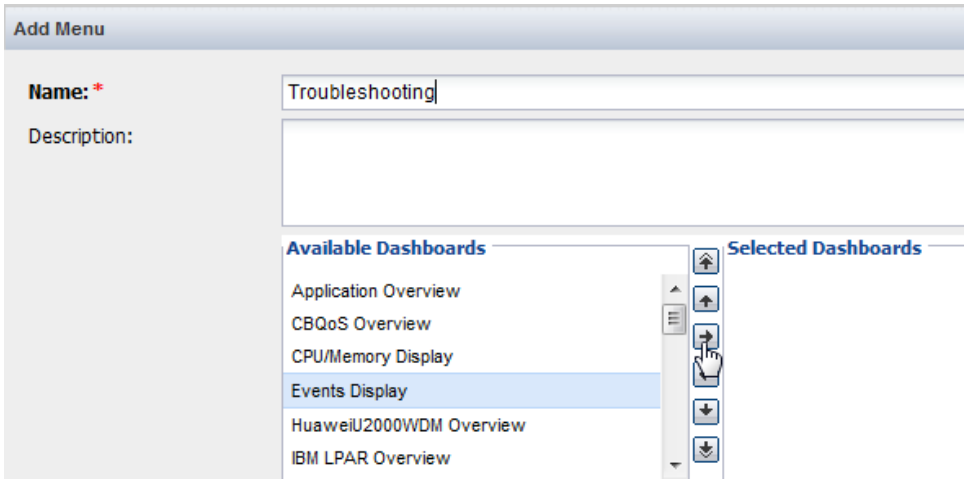
   The Add Menu page opens.
4. Supply values in the following fields:

   Name

   Is a name for the menu. This name appears when you click the Dashboards tab.

   Description

   (Optional) Describes the menu to help other operators identify it.
5. Select a dashboard in the Available list that you want to include in the menu.



6. Click the right arrow.

   The dashboard moves to the Selected 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.

7. Click Save when you have finished creating menus. Or click Save & Add Another to save the menu and add another menu.

Edit a Menu

Administrators and designers can edit menus to meet changing needs and new job responsibilities for CA Performance Center operators. They can edit custom or factory menus by adding new dashboards, removing dashboards, and changing their order.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Menus page (see page 149).

   The Manage Menus page displays the current list of menus.
3. Select the menu that you want to modify, and click Edit.
4. Modify menu settings as required.

   For example, to remove a dashboard from the menu, take the following steps:

   - Select it where it appears in the Selected list.
   - Use the arrow button to move it to the Available list.

   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.
5. Click Save.

   The menu is edited.

Delete a Menu

When a menu is no longer being used, you can delete it.

Note: Deleting a user account that is associated with a custom menu does not delete that menu.

Follow these steps:

1. Log in as a user with the required administrative role rights (see page 70).
2. Navigate to the Manage Menus page (see page 149).

   The Manage Menus page displays the current list of menus.

3. Select the menu that you want to delete, and click Delete.

   The Delete Menu dialog opens.

4. Click Yes to confirm the deletion.

   The menu is deleted and no longer appears on the Dashboards tab when the associated user logs in. Any dashboards that are contained in the menu definition are not affected and can be added to other menus.

Chapter 8: Administration with Web Services

This section contains the following topics:

CA Performance Center Web Services

CA Performance Center offers a set of APIs that let you automate provisioning and configuration tasks. The most frequently repeated or time-consuming tasks are exposed to you by means of web services.

Some of these APIs consist of RESTful web services. *REST*, or Representational State Transfer, refers to a method of structuring software for the World Wide Web or other applications that conform to the requirements of HTTP in client-server networks. The REST model lets you access a set of resources by means of a fixed set of operations. This model takes advantage of widely deployed HTTP features that are supported by common hardware, such as gateway devices.

The CA Performance Center RESTful web services can programmatically perform the following tasks:

- Create user accounts
- Create containers for MSP customer sites ("tenants")
- Load a list of groups from an XML file
- Create, edit, and delete SNMP profiles
- Create IP domain definitions and associate them with tenants
- Provide lists of all configuration items, such as custom user accounts, roles, or groups, that are already in the system

Additional APIs let you create custom data views and run custom database queries to gain access to precise data sets and build new dashboards. For more information, see the *RIB API User Guide*. And a SOAP API lets you change settings in the Single Sign-On authentication component.

Basic Operations in REST Web Services

The REST specification leaves room for some flexibility. As a result, RESTful web services can use basic HTTP syntax to perform different tasks.

In this implementation, the basic REST commands are used as follows:

- GET - Log in or retrieve information from a server database. Only requires a browser session.
- POST - Create an object. Often requires XML input to supply parameters.
- PUT - Edit an existing object. Occasionally also used to create an object. Usually does not require XML input to supply parameters.
- DELETE - Delete an existing object.

Here is an example of a simple operation:

```
http://[server IP address]:8181/pc/center/webservice/tenants/
tenantName/{tenantName}/description/{NewDescription}
```

This operation is a PUT that updates the description parameter of a tenant.

You would substitute the desired values inside the braces { } for the required parameters:

{tenantName}

The name of the tenant that you want to edit.

{tenantDescription}

The new description to identify this tenant.

The method 'get id names' gets a list of supported ID names. For example, you would enter the following commands for the tenant web service:

```
http://[server IP address]:8181/pc/center/webservice/
tenants/idNames
```

The following list is returned:

```
[tenantAccountId, tenantItemId, tenantName]
```

Each request receives a reply consisting of an HTTP status code, which indicates the type of problem, and HTTP status response text to describe the problem. The following HTTP response code ranges are used for feedback:

- 200 - Command status is 'OK'.
- 400 - A user error has occurred. Errors in this range indicate a problem with the input text (400) or the user credentials (403) and can usually be easily corrected.
- 500 - An system error occurred. Errors in this range typically indicate a system fault. Such errors can require assistance from CA Technical Support to resolve them.

For more information about HTTP status codes, see the following IETF website:

http://www.ietf.org/rfc/rfc2616.txt

Accessing the API

API components are automatically installed with the CA Performance Center software. You can run the web services from a web browser. The launch page includes a list of the available web services, endpoint addresses, and WADL and WSDL URIs.

Access the launch page using the following URL syntax:

```
http://[server IP address]:8181/pc/center
```

If you use a testing utility to run web service calls, you receive feedback that is useful for debugging purposes. For example, you can test your scripts using the soapUI open source testing utility. Using a testing utility is also a timesaver. You can supply username and password parameters as service endpoints for automatic authentication of all service calls.

Such utilities require a WSDL file (an XML file that conforms to the Web Services Description Language) that describes the service being tested. In the REST format, the simpler Web Application Description Language (WADL) is used instead. The CA Performance Center API launch page gives you access to a WADL file for each web service that you can use for testing. A link to the WSDL is provided for the SOAP web services.

Finding Out More

The web services provide their own documentation, including lists and descriptions of the available parameters and operations. The documentation is accessible in HTML format from the API launch page:

```
http://[server IP Address]:8181/pc/center/rest
```

where the server IP address is the same as the CA Performance Center server.

A use case to help you get started creating tenants and users by deploying web services is also available on the documentation bookshelf.

Chapter 9: 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 the relevant service (or daemon). Find log files in the following path:

`CA/PerformanceCenter/<servicename>/logs`

where the *servicename* is one of the following:

DM

Is the Device Manager.

EM

Is the Event Manager.

PC

Is the main console program.

SSO

Is the Single Sign-On authentication software. 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 associated with 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. Log in as a user with administrative privileges.

   Change directories to the directory that corresponds to the desired service.

   ```
   /opt/CA/PerformanceCenter/DM/etc/
   ```

2. Open the log configuration file named log4j.xml.
3. Locate the 'root' element near the end of the file to change the global server logging level.
4. Change the value for the root level element to one of the following:
   - FATAL
   - ERROR
   - WARN
   - INFO
   - DEBUG
5. Locate the relevant 'logger' element in the same file to change the logging level for a particular category.
6. Change the value of the level element to one of the values listed previously (that is, FATAL, ERROR, and so on).

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. Log in to or use Remote Desktop to access the CA Performance Center server.

   On Linux, log in as root.

2. Change to the log directory for the relevant service:

   `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 you supplied 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 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 161).

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 22)

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 22).

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 might have 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.

More information:

Synchronization (see page 18)
View the Data Source Log (see page 22)
Data Source Registration Failed (see page 161)

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 161).
- Data source synchronization failed. For more information, see Data Source Synchronization Failed (see page 163).

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 59).

Also make sure that you have not logged in as a user associated with the Default Tenant. This tenant typically sees no managed items.

Glossary

Context pages

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.

dashboards

Dashboards are 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.

data source synchronization

Data source synchronization occurs when a data source is first registered to CA Performance Center. It 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.

data sources

Data sources are the supported products that provide performance and configuration data to CA Performance Center. Data source products, which perform monitoring, data collection, and data aggregation, can often function independently. However, once they are registered to an instance of CA Performance Center, they are called data sources.

Default Tenant Administrator

The *global administrator* administers product settings for all tenants. This user account, also called the "Default Tenant administrator" because of its association with the Default Tenant, creates tenants and performs tenant configuration.

domain

IP domains are logical groupings that identify data collected 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.

drill down

To *drill down* means to navigate from one data view or dashboard in CA Performance Center to another, more detailed data view or context page. The new page displays data from the same timeframe, for the same managed item or set of items.

global synchronization

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.

group

A *group* is a filter definition that functions as a container for managed items. Groups let you logically organize managed items in a tree structure, with each group containing subgroups or managed items. The structure is propagated to the data sources, where it enables drilldown from top-level groups into data from an increasingly narrow but related context.

Host

The *host* corresponds to the main CA Performance Center Administrator. In many cases, the host represents the managed services provider whose IT staff are managing and monitoring the networks and systems of multiple customers. Each host contains multiple user accounts for IT staff members, as well as its own grouping structure to organize managed items from shared infrastructure. A host can manage the domains and infrastructure of multiple tenants.

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.

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.

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.

reports

Reports describe the output from an exported dashboard page. Reports contain the same data and information as the associated dashboards, but they are formatted to meet the requirements of the export destination. You can print reports, send them by email, or export them in PDF format.

REST

REST, or Representational State Transfer, refers to a method of structuring software for the World Wide Web or other applications that conform to the requirements of HTTP in client-server networks. The REST model lets you access a set of resources by means of a fixed set of operations. This model takes advantage of widely deployed HTTP features that are supported by common hardware, such as gateway devices.

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. In a well-planned deployment, roles let users access dashboards that they require to perform their duties and restrict access to features that they do not require.

shared dashboard

A *shared dashboard* is a page that is included in a shared menu—any menu other than the My Dashboards menu, whose contents are specific to user accounts.

Single Sign-On

Single Sign-On is the term used to describe the authentication scheme used by CA data sources that CA Performance Center supports. The Single Sign-On component provides the login page that supports user authentication in CA Performance Center and in the data source products. Once users are authenticated to CA Performance Center, they can navigate among CA Performance Center and registered data sources without signing in a second time.

site groups

Site groups are custom groups that are based on physical locations, such as a city, region, office, or campus. Typically, they contain items and subgroups of items that are grouped by location. When you add site groups to the other custom groups in your tree structure, you can build reports that are organized both geographically and logically.

SNMP profiles

SNMP profiles are definitions that contain the information necessary to enable secure queries of device MIBs using SNMP.

Summary pages

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.

tab

Tabs are the prominent links across the top of the CA Performance Center interface that let you view dashboards and open administration tools. For example, the Dashboards tab lets you select a dashboard page to view from a menu.

tenant

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.

tenant administrator

A *tenant administrator* has permissions to view all data from a single tenant. The tenant administrator can also add configuration, such as group definitions, profiles, and user accounts, to this tenant. This administrator role does not have permission to view items associated with any other tenant.

view

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.

Index

V