CA Performance Center

Managed Service Provider Guide

2.4.1

ca technologies

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Introduction 7

Chapter 2: Creating and Managing Tenants 23

Chapter 3: Deploying Grouping Strategies 37

Chapter 1: Introduction

This section contains the following topics:

Managed Service Providers and CA Performance Center

CA Performance Center supports monitoring in managed-service and other hosted environments. The multi-tenancy feature lets you create multiple customers and monitor their environments separately.

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.

At every level, the distinction between two of these customers (tenants*)* is complete. The users assigned to a tenant cannot see data from other tenants. Any users within the tenant who have administrative privileges can only view and modify configuration within that same tenant.

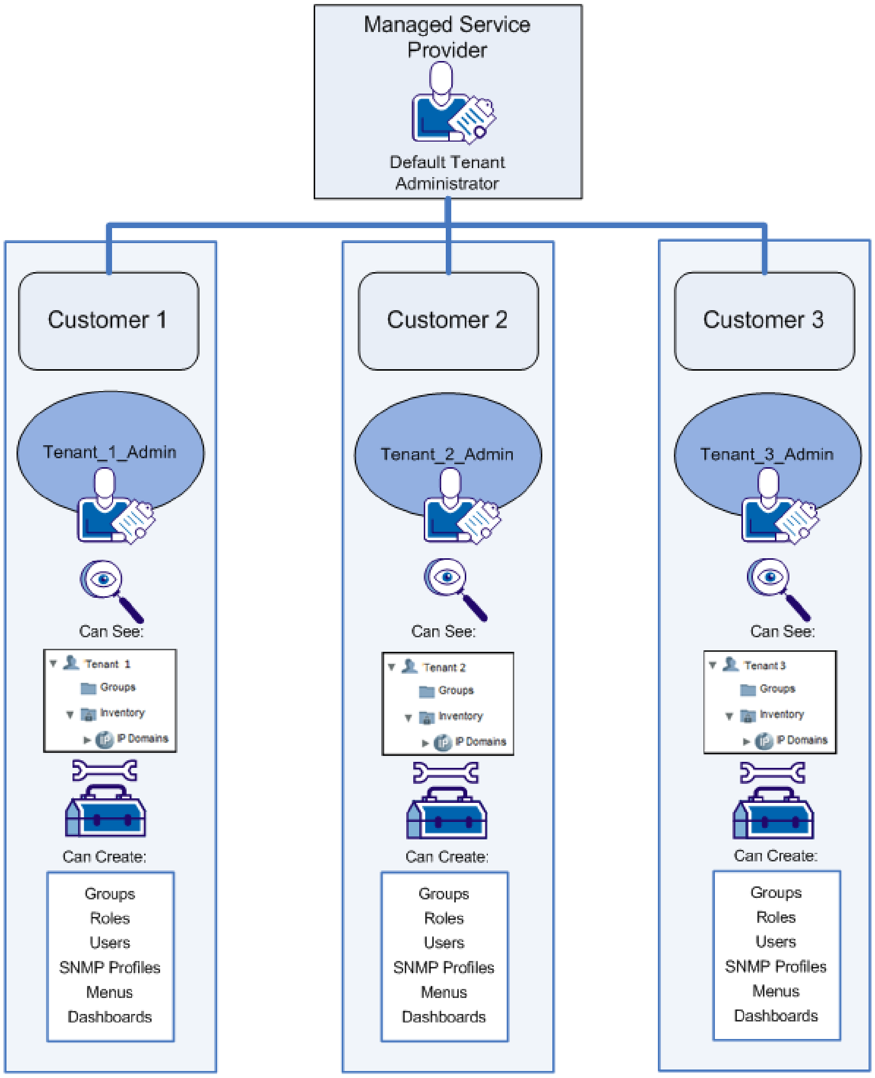
Although settings and data are not shared among tenants, they can be viewed by the main product administrator. The *global administrator* administers product settings for all tenants. This user account, also called the "Default Tenant administrator" because of its association with the Default Tenant, creates tenants and performs tenant configuration. The Default Tenant Administrator typically represents the MSP itself.

Administrator Roles for Multi-Tenancy Support

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

- Global Administrator (see definition on page 49) - 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 50) - 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 24)
Administer a Tenant (see page 28)

Understanding Deployment Options

Several important factors must shape your deployment plans. Do not create tenants or IP domain definitions without a solid understanding of the following factors:

- The size, scope, and organization of your monitoring environment
- The CA data sources that you plan to install and register
- Data source support for the multi-tenancy features in CA Performance Center

All of these factors work together to determine your strategy. For example, some data sources do not detect IP domains that are created within tenants.

When planning multi-tenancy configuration options, keep in mind that once data collection has started, it is much more difficult to change IP domain or tenant definitions. The data that CA data sources collect and aggregate retains a database association with the original IP domain or tenant.

We strongly recommend reading Data Source Support for Multi-Tenancy (see page 9) and Domain Monitoring Considerations (see page 11) and understanding those guidelines before you create tenants or IP domains.

Data Source Support for Multi-Tenancy

Support for multi-tenant monitoring in CA Performance Center is subject to some limitations in the registered data sources. Where a Data Aggregator data source has fully implemented multi-tenancy and IP domain monitoring, the following data sources offer more limited support:

- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Spectrum
- CA eHealth
- CA Application Performance Management

The following table summarizes data source support for multi-tenant deployment features:

Data Source	Features Supported	Notes
Data Aggregator	All: ■ IP Domains ■ Default Tenant configuration (such as tenant groups and SNMP profiles) ■ Default Tenant ownership of managed items ■ Custom Tenant configuration and ownership of managed items	Full support for all multi-tenancy features.
CA Network Flow Analysis	All.	Assign a tenant and IP domain to each Harvester and router. Tenant assignment determines the configuration items that are available (such as tenant SNMP profiles). A few limitations are noted in Other Deployment Considerations (see page 13).
CA Application Delivery Analysis	■ IP Domains ■ Custom Tenant configuration	Does not segregate data within the data source interface.
CA Spectrum	All. However, tenancy is only visible in the CA Performance Center interface, not in OneClick.	OneClick receives IP domains from CA Performance Center. Models in IP domains are synchronized them with CA Performance Center (and thus, associated with custom tenants).
CA Unified Communications Monitor	All.	Locations are automatically associated with IP domains by their subnets.

Data Source	Features Supported	Notes
CA eHealth; CA Application Performance Management	None.	All items from these data sources are associated with the Default Tenant and Default IP Domain. Add items from these data sources to Service Provider groups to grant tenant access to them.

Notes:

CA Application Delivery Analysis monitors IP domains without a concept of tenants. As a result, CA Performance Center receives all items from CA Application Delivery Analysis in the Default Tenant. However, CA Application Delivery Analysis does support IP domains. CA Performance Center can thus associate these items with tenants according to their IP domain. Be aware that some managed items are duplicated between the Default Tenant and custom tenants.

Starting with r9.3, CA Spectrum supports custom IP domains. CA Spectrum devices can be placed in custom IP domains or in the Default IP Domain. Tenants are not visible in CA Spectrum OneClick. However, tenants in CA Performance Center have associated CA Spectrum devices based on IP domain. The global administrator can also make these items available for monitoring by tenant users by placing them into the Service Provider Items group. For more information, see the *CA Spectrum-CA Performance Center Integration Guide*.

Domain Monitoring Considerations

The IP domains feature supports environments where multiple enterprise systems must be monitored separately. For example, a managed services provider wants to monitor the systems and networks of different customers separately. The MSP administrator creates a tenant in CA Performance Center for each customer enterprise. The data and the configuration for each tenant are hidden from all other tenant users.

However, in other situations, you can deploy multiple IP domains in CA Performance Center without multi-tenancy. In other words, some deployment models consist of *multiple IP domains within the Default Tenant*.

The IP domain lets you control data collection parameters. Use custom IP domains to determine which collection devices monitor the managed items in your infrastructure. Each collection device, such as a Data Collector or a CA Unified Communications Monitor Collector, operates within a single IP domain.

The following list provides some examples of environments where you can deploy multiple IP domains within the Default Tenant:

- A deployment that includes a CA Application Delivery Analysis data source.

  CA Application Delivery Analysis monitors IP domains without a concept of tenants. The IP domains that you create within custom tenants are not detected. When Data Aggregator or CA Network Flow Analysis monitors items within those domains, they appear as duplicates in CA Application Delivery Analysis. The duplicate data is not aggregated.

- A large deployment that requires load balancing.

  For example, your enterprise includes ten routers with many interfaces, IP SLA testing, and QoS policies in place. Such a deployment would have a polling load similar to an environment with hundreds of servers being monitored for CPU and memory statistics only.

  To monitor the busy routers, you can create an IP domain and can deploy a powerful system for the Data Collector within that domain. And you can monitor the servers in another IP domain, using a less powerful system for the Data Collector. By running discoveries in the appropriate IP domains, you can determine the devices that each Data Collector is polling.

- A method to minimize the potential network impact of bulk statistics collection.

  For example, you can deploy a Data Collector close to the devices that it is monitoring. The Data Collector can process a massive amount of bulk statistics and can reduce them to a much smaller set of monitored metrics, which it then sends to the Data Aggregator. As a result, less data passes across the network between the two components.

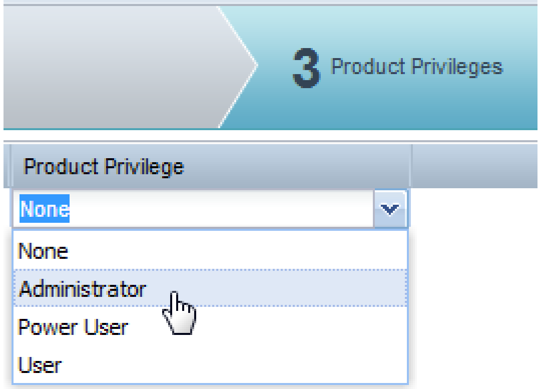
- Isolation of potentially sensitive SNMP traffic to a specific area, such as a DMZ.

  For example, security policies do not let SNMP traffic travel across the router that limits an area of network. One option is to deploy a Data Collector behind the router. A path to return the processed metrics back to the Data Aggregator must be open.

  The metric data traveling between the components is not encrypted. However, it is packaged and compressed in a way that makes it less "sniffable." As a result, the data is more secure than raw SNMP flows. To accomplish this setup, create an IP domain for the DMZ and deploy a Data Collector within that IP domain.

Other Deployment Considerations

As indicated in the diagram in Data Source Support for Multi-Tenancy (see page 9), CA Network Flow Analysis supports the multi-tenancy features in CA Performance Center. However, take care when selecting user account product privileges. The product privilege to a data source enables a user to drill down from a view in CA Performance Center back to the source of the data.



Assuming that you have carefully segregated data from different customer environments into separate tenants, you probably want to prevent users from returning to the CA Network Flow Analysis interface. In that interface, tenant separation is not applied for users at the Administrator and Power User level—all data is available for viewing in reports. Product privileges are set in the Add or Edit User Account wizard.

Important! Assign the 'User' product privilege to any user who does not require access to all data in the CA Network Flow Analysis data source.

Another point to consider is the 'Manage Reports' role right for CA Network Flow Analysis. A user who has this role right can view all data in the CA Network Flow Analysis console.

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 15) 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.

About Tenants

By default, all managed items and their data are associated with the Default Tenant. Adding custom tenants to CA Performance Center lets you create separate CA Performance Center monitoring environments that you administer from a single user interface. A *tenant* represents a customer environment that a managed service provider administers. Each tenant environment is independent and effectively functions as a separate instance of CA Performance Center. Each instance can contain multiple users and roles that are not shared among tenants.

The basic tenant definition contains a few parameters to identify the MSP customer and let other operators access managed items and configuration for the customer. Each tenant must contain at least one IP domain (see definition on page 49). You or the tenant administrator can then set up as many of the following definitions as required to manage the enterprise infrastructure and applications:

- SNMP profiles
- Additional user accounts
- Roles
- Custom groups
- Custom dashboards
- Custom menus

Custom IP domains (see page 20) 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.

Creating and Managing Groups

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

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

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

More information:

Create a Custom Group (see page 41)
Groups for Multi-Tenant Deployments (see page 18)

System Groups

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

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

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

Inventory ▶ 🔒

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

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

Collections ▶ 🔒

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

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

Special groups for multi-tenant deployments also appear after you create at least one custom tenant. For more information, see Groups for Multi-Tenant Deployments (see page 18).

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

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

All Items ▶ 🔒

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

Data Sources

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

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

IP Domains

Includes all of the custom IP domains created by the administrator. Also includes the Default Domain, which contains all items that are not explicitly assigned to a custom domain. For more information, see IP Domains (see page 19).

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.

Groups for Multi-Tenant Deployments

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

Defined Tenants

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

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

Service Provider Global Groups

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

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

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

Domains

Includes all of the custom IP domains that are used to associate managed items with tenants. Also includes the Default Domain, which contains all items that are not explicitly assigned to a custom domain. For more information, see IP Domains (see page 19).

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

Groups (Tenant)

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

Inventory (Tenant)

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

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

IP Domains

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

Service Provider Defined Groups

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

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

Service Provider Items

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

IP Domains

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

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

Administrators and Designers can create custom dashboards to monitor activity on a specific domain or group of domains. Service provider administrators (that is, global administrators (see definition on page 49)) can see data from all IP domains. But they can create user accounts that have permission to see data from a single customer domain.

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

About IP Domains

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

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

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

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

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

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

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

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

More information:

Set Up Tenant IP Domains (see page 27)
Associating Items with IP Domains (see page 21)
IP Domains (see page 19)
How IP Domains are Configured (see page 21)

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 23).
2. Create custom IP domains for each tenant. For more information, see Set Up Tenant IP Domains (see page 27).
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.
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 21).

   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.

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 21).

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

Chapter 2: Creating and Managing Tenants

This section contains the following topics:

How to Set Up a Tenant

A global administrator must perform the initial steps to set up a multi-tenant deployment in CA Performance Center. A global administrator is associated with the Default Tenant and has access to all tenant configuration parameters. The predefined Administrator role enables global administrator access for a user account.

Before you create a tenant in CA Performance Center, we recommend working closely with the customer. Collect some basic information about the customer environment. For example, you need to know the IP domains to be monitored for this customer. Some knowledge of physical and virtual system topology is useful for creating a custom grouping structure to represent the customer environment.

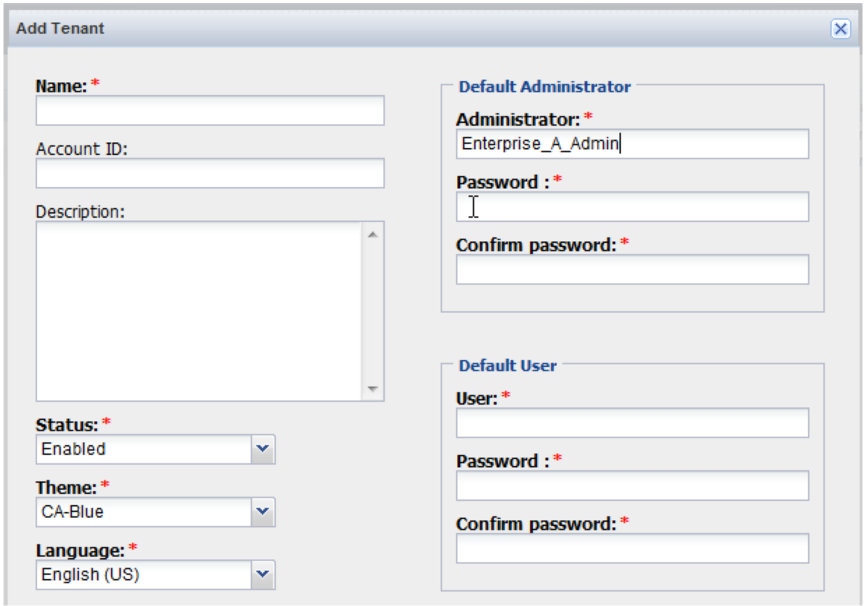
Select a user to act as the tenant administrator. This person should have broad knowledge of the customer systems and networks. The designated tenant administrator can then complete the tenant configuration by creating custom groups, roles, users, SNMP profiles, menus, and dashboards.

To set up a new tenant, take the following steps:

1. Obtain a list of the IP domains and SNMP communities on the customer networks.
2. Designate a user to act as tenant administrator. For example, select a representative of the customer site that is monitored.

3. Add a tenant definition.

   As part of tenant creation, you also create a tenant user account with administrative privileges.



Add Tenant

Name: *

Account ID:

Description:

Status: * Enabled

Theme: * CA-Blue

Language: * English (US)

Default Administrator

Administrator: * Enterprise_A_Admin

Password : *

Confirm password: *

Default User

User: *

Password : *

Confirm password: *

4. Administer the tenant: temporarily log in as the tenant administrator by setting the tenant scope.

5. Create at least one IP domain for the tenant.

6. Create at least one SNMP profile to provide SNMP access to devices in the tenant environment.

   Note: If data collection is already taking place, tenant system groups will be automatically created and populated with data from this domain. With groups already available, you can allocate access permissions to tenant users.

The designated tenant administrator can then log in. This user can set up all other tenant configuration (any custom groups, roles, users, menus, and dashboards that the tenant requires).

Add a Tenant

Only a user with the predefined Administrator role (a "global" administrator) can add tenant definitions to distinguish among customer networks and systems. This user is equivalent to the tenant administrator for the Default Tenant.

During tenant creation, you can also create a tenant administrator and a tenant user. Unlike the global administrator, the tenant administrator (see definition on page 50) 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 feature.

Follow these steps:

1. Log in as a user with the predefined (global) Administrator role.

   Note: A tenant administrator cannot create tenants.

2. Navigate to the Manage Tenants page.

   The page displays the current list of tenants.

3. Click New.

   The Add New Tenant page opens.

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

   Name

   Is a name for the tenant.

   Account ID

   Identifies this tenant; usually corresponds to the MSP account number.

   Description

   (Optional) Describes the tenant.

   Status

   Is the status of this tenant. Select one of the following options:

   - Enabled: Enables tenant user accounts for use.
   - Disabled: Prevents any actions by user accounts that are associated with this tenant.

   Theme

   Specifies the format—the theme that controls the appearance of the page in the browser window—to use for this tenant. All operators whose user account is associated with this tenant see this same theme.

   Language

   Specifies the language (locale) for this tenant. Select a language from the list.

5. Create the tenant administrator account for this tenant. Enter information for the following parameters:

   Administrator

   Is a login name for the tenant administrator account.

   Password

   Defines a password for the user account. The password is limited to 32 characters.

   Confirm Password

   Confirms the password.

6. Create the tenant user account. The associated operator can access tenant-specific dashboards, but cannot access any administration functions.

7. Click Save.

   The new tenant definition is created, but it lacks required parameters, such as IP domains. For more information, see Set Tenant Scope (see page 26).

More information:

Administrator Roles for Multi-Tenancy Support (see page 7)

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).

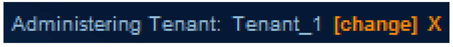
2. Navigate to the Manage Tenants page.

   The page displays the current list of tenants.

3. Select the tenant that you want to administer.

4. Click Administer.

   The Administering Tenant indicator appears at the top right to show that you are administering the selected tenant environment.

   Administering Tenant: Tenant_1 [change] X

   You are only able to see the configuration associated with the selected tenant.

   You can now create the IP domains, SNMP profiles, roles, users, menus, and groups that are required to represent and monitor this tenant environment. Use the menus under the Admin tab to configure the tenant.

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

   You return to the Manage Tenants page, where you can select another tenant.

6. Exit a tenant scope by clicking the X next to the tenant indicator.

Set Up Tenant IP Domains

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

After you create a tenant definition, add all IP domains containing the tenant's managed devices.

Data sources classify managed items into IP domains using different methods. Typically, domain identifiers do not appear in the data source until you have created at least one custom domain in CA Performance Center.

Follow these steps:

1. Log in as a tenant administrator for the selected tenant.

   Or set the tenant scope (see page 26) to access tenant configuration as a global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, Custom Settings, and click IP Domains.

   The Manage IP Domains for [Tenant Name] page opens.

3. Click New.

   The IP Domains Administration dialog opens.

4. Supply information for the required parameters.
5. Click Save.

   The new IP domain appears in the list, which is scoped to the current tenant.

   Repeat the steps as required to add more domains to this tenant.

Set Up Tenant SNMP Profiles

A tenant definition can contain one or multiple SNMP profiles, which are used to contact devices in the tenant enterprise systems using SNMP. Operators who are logged into one of the tenant user accounts only have permission to view the SNMP profiles that were created for that tenant.

Follow these steps:

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

   Or set the tenant scope (see page 26) 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 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.

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.

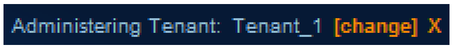
When the tenant scope has been set, the procedures for administering a tenant are identical to the procedures to perform in a single-tenant environment.

Follow these steps:

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

   Or set the tenant scope (see page 26) 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.

   Administering Tenant: Tenant_1 [change] X

   You can now see and modify only definitions associated with this tenant.

2. Click the Admin tab, and select an item to modify:
   - IP Domains
   - SNMP Profiles
   - Groups
   - Menus
   - Roles
   - Users
3. Follow the procedures specific to the selected item.
4. Save your changes.

   The modifications are only apparent to administrators and to operators whose user accounts were created within this tenant environment.

More information:

Set Up Tenant IP Domains (see page 27)
Set Up Tenant Roles (see page 32)
Set Up Tenant Users (see page 34)
Set Up Tenant Groups (see page 30)
Set Up Tenant SNMP Profiles (see page 28)
Set Up Tenant Menus (see page 31)

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 26) 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.

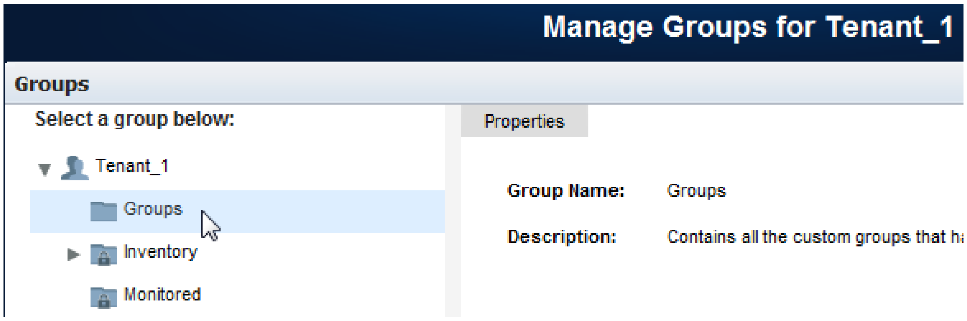
   The Manage Groups for [Tenant Name] page opens.

   When scoped to a tenant, the top-level node in the Groups tree is a system group (see page 16) 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.



Group Name: Groups

Description: Contains all the custom groups that h

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 45) by adding items in the Manage Groups interface.
   - Create rules (see page 43) to manage group membership

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 26) to access tenant configuration as a global administrator, and then proxy a tenant administrator associated with this tenant.

2. Select Admin, User Settings, and click Menus.

   The Manage Menus for [Tenant Name] page opens.

   The page displays the current list of menus for this tenant.

3. Click New.

   The Add Menu page opens.

4. Type a Name for the menu. This name appears in the floating menu when you click the Dashboards tab.

5. (Optional) Type a Description of the menu to help other operators identify it.

6. Select a dashboard in the Available Dashboards list.

7. Click the right arrow.

   The dashboard moves to the Selected Dashboards list.

   Use Shift + Click or Ctrl + Click to select multiple dashboards. Use the up and down arrows to change the order of the dashboards in the menu.

   Note: A maximum of 20 dashboards can be assigned to a single menu. An error message appears if you try to add more than 20 dashboards.

8. Click Save to save the new menu. Or click Save and Add Another to create more menus.

   When users associated with this tenant log in, they see the new menu on the Dashboards tab. Users associated with other tenants do not see it.

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 7).

Follow these steps:

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

   Or set the tenant scope (see page 26) 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.

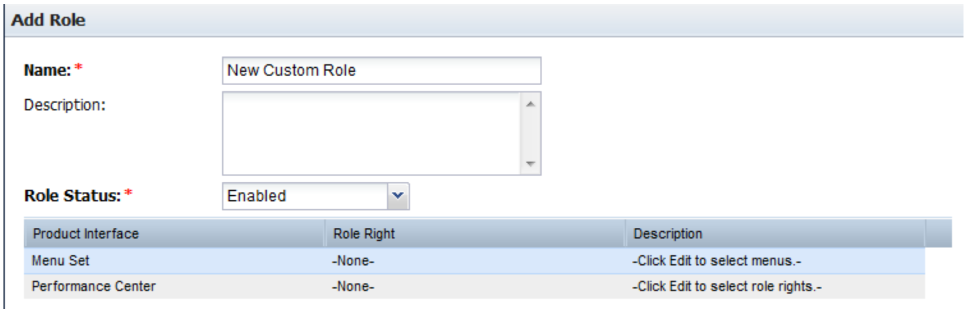
   Description

   (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.



Add Role

Name: * New Custom Role

Description:

Role Status: * Enabled

Product Interface	Role Right	Description
Menu Set	-None-	-Click Edit to select menus.-
Performance Center	-None-	-Click Edit to select role rights.-

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.

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 26) to access tenant configuration while logged in as a global administrator.

   The Administering Tenant indicator appears to show that you are administering the selected tenant environment.

2. Select Admin, User Settings, and click Users.

   The Manage Users for [Tenant Name] page opens.

   The page displays the current list of user accounts for this tenant.

3. Click New.

   The Create New User wizard opens.

4. Enter information for the required account parameters:

   Name

   Is a login name for the user account. Limited to 50 characters.

   Description

   (Optional) Describes the user account to help you identify it.

   Email Address

   (Optional) Associates an email address with the user account.

   Preferred Language

   Specifies the language spoken by the operator associated with the user account.

   Authentication Type

   Identifies the authentication method that applies to this user account. The method must match Single Sign-On configuration. Select one of the following:

   - Performance Center—The default authentication scheme deployed by CA Performance Center.
   - External—A third-party authentication scheme, such as LDAP or SAML.

   Password

   Defines a password for the user account. The password is limited to 32 characters.

   Time Zone

   Corresponds to the time zone in which the user will view data.

   Default: UTC (Coordinated Universal Time).

   Role

   Is the role assigned to the user account.

   Account Status

   Determines whether the account is enabled for use (activated).

   Other account parameters do not apply to user accounts that are scoped to a tenant.

5. Click Save.

   The new user account is saved as part of the tenant definition. Any operator who logs in with this user account only sees dashboards and data from managed items in the IP domains associated with this tenant.

Chapter 3: Deploying Grouping Strategies

This section contains the following topics:

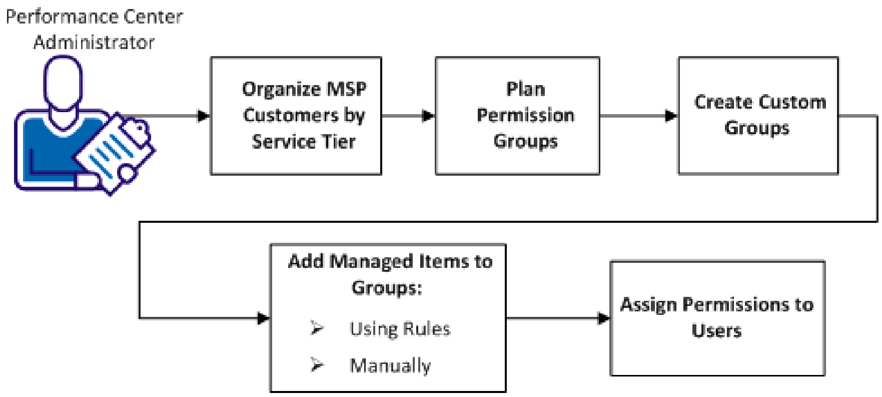
Creating Custom Groups to Monitor MSP Customers

You are a manager for a large managed service provider (MSP). You have Global Administrator (see definition on page 49) access to CA Performance Center. You have registered data sources to monitor infrastructure usage, status, and performance at each customer site. In your role as CA Performance Center administrator, you can now create custom groups to organize infrastructure monitoring and reporting.

Custom CA Performance Center groups support the monitoring and management tasks of the IT organization. Custom groups let you organize managed items to facilitate troubleshooting and optimize reporting. Groups also let you assign data access permissions to IT staff. Using permission groups, you can make sure that the team monitoring selected devices or systems can see their performance data.

An MSP deployment represents some unique requirements. At the MSP level, you can create container groups that correspond to broad customer traits. You can use these groups to assign permissions to your IT staff and dedicate IT resources to address problems affecting individual MSP customers.

Group creation involves planning, creating, and populating groups, and then assigning groups as permissions to user accounts.


Performance Center Administrator
Organize MSP Customers by Service Tier
Plan Permission Groups
Create Custom Groups
Add Managed Items to Groups:
➢ Using Rules
➢ Manually
Assign Permissions to Users

Tasks
Organize MSP Customers by Service Tier (see page 38)
Plan Permission Group Assignments (see page 40)
Create Custom Groups (see page 41)
Add Managed Items to Groups Using Rules (see page 43)
Add Managed Items to Groups Manually (see page 45)
Assign Permissions to Users (see page 47)

Organize MSP Customers by Service Tier

Before you create custom groups to monitor MSP customer systems, plan the groups by organizing the customers by their tier of service. Organization into categories lets you approach group creation with a strategy in mind. For more information, see MSP Grouping Strategies (see page 39).

Typically, MSP customers subscribe to different service tiers. Assume, for example, that you and your team are responsible for the following categories of customers:

- Tier 1 - This category represents the highest tier of managed services. The MSP must provide continual monitoring of all data centers and quality of service (QoS) on all routers. This category also contains other stringent service-level agreements (SLAs), including rapid problem resolution.
- Tier 2 - This category represents the next-highest tier of managed services. The MSP must provide continual monitoring of key data centers, rapid problem resolution, and QoS in selected data centers.

Follow these steps:

1. Make a list of customer systems for which your team of IT staff is responsible.
2. Obtain a list of subscribers for each tier of service that your MSP organization offers.
3. Make another list, placing the customers whose systems your team monitors into categories based on their subscription.

For example, if you have responsibility for six MSP customers, you can organize them in two categories as follows:

Tier 1:

- Customer A
- Customer B
- Customer C

Tier 2:

- Customer D
- Customer E
- Customer F

This list helps you plan custom groups to organize customer data and assign permissions to IT staff.

MSP Grouping Strategies

Organizing groups of managed items by customer level of service is an appropriate strategy for Managed Service Providers for several reasons. For example, if your staff monitors MSP customers subscribing to Tier 1 and Tier 2 levels of service, you can create a group to represent each tier. You can then create subgroups to represent each customer and place managed items in these subgroups.

With separate groups for each tier of service, you can assign dedicated staff to monitor the customers in each tier. Application, server, and network specialists with user access to CA Performance Center data can be assigned to each tier.

Any issues affecting a customer are reported up, at the level of the service tier group. You can set up automatic notifications based on these groups so that the appropriate team receives the alerts. If the same IT professionals monitor additional tiers, more stringent expectations for performance metrics can be applied to customers with more stringent SLAs.

Tiered grouping can be extended. CA Performance Center users commonly create subgroups based on the geographical locations of sites and devices. You can place geographical subgroups within the groups representing service tiers. If geography is not a concern, you can create custom subgroups that organize critical infrastructure components.

You can also compose subgroups based on priority, or on dependencies, such as a critical application server that depends on selected router uplinks. Any subgroups you create can be added to the larger 'Tier 1' and 'Tier 2' container groups so that alerts are reported for the associated tier.

Plan Permission Group Assignments

Plan a strategy for assigning custom groups as permissions to CA Performance Center operators.

Permission groups are custom groups that organize managed items for purposes of data access. They are called custom groups until they are assigned to user accounts as permission sets.

Assigning custom groups as permissions has the following benefits:

- Lets users view data specifically within their area of responsibility
- Lets administrators restrict the users who can view data for security reasons

Follow these steps:

1. Make a list of MSP employees who will use CA Performance Center when it is fully deployed.

   Note: Each CA Performance Center operator requires a user account. User accounts should not be shared.

2. Use your list of MSP customers to organize staff assignments. For more information, see Organize MSP Customers by Service Tier (see page 38).

   You can create a table to organize assignments. For example:

IT Staff Members	Current Customer Assignments	Customer Service Tier
Staff Member 1 and Staff Member 2	Customer A	Tier 1
Staff Member 3	Customer B	Tier 1
Staff Member 4	Customer C	Tier 1
Staff Member 5	Customer D	Tier 2
Staff Member 6	Customer E	Tier 2
Staff Member 7	Customer F	Tier 2

If multiple staff members are assigned to the same customer, they require the same permission group assignments.

3. Use the table you created to determine what permission groups are required to monitor all customers.

   In this example, you need two permission groups: Tier 1 and Tier 2. You can add managed items from all customer systems to these two custom groups.

4. Make a list that maps staff members to permission groups.

   The resulting list guides you when you create groups and assign them as permissions to user accounts. For example:

IT Staff Member	Permission Group
Staff Member 1	Tier 1
Staff Member 2	Tier 1
Staff Member 3	Tier 1
Staff Member 4	Tier 1
Staff Member 5	Tier 2
Staff Member 6	Tier 2
Staff Member 7	Tier 2

Create a Custom Group

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

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

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

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

Follow these steps:

1. Log in as a user with the required administrative role rights.

2. Navigate to the Manage Groups page.

   The page displays current groups in a tree structure.

3. To find a location for the new group, expand the nodes in the Groups tree.

4. Right-click the node, and select Add Group.

   The Add Group window opens.

   The New tab is selected by default.

5. Supply values for the following parameters:

   Group Name

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

   Description

   (Optional) Helps you identify the group.

6. Confirm the setting for the following parameter:

   Include the children of managed items

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

   Default: Selected.

7. Select Custom from the Group Type list.

8. Click Save.

   The new group appears in the Groups tree.

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

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

More information:

Add Managed Items to a Group Manually (see page 45)
Add Managed Items to a Group Using Rules (see page 43)

Add Managed Items to a Group Using Rules

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

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

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

Note: Group rules do not apply to domain groups.

Follow these steps:

1. Navigate to the Manage Groups page.

   The page displays current groups in a tree structure.

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

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

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

3. Click the Properties tab in the right pane.

   The Properties page opens.

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

   Include the children of managed items

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

5. Click Save.

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

   The Add Rule dialog opens.

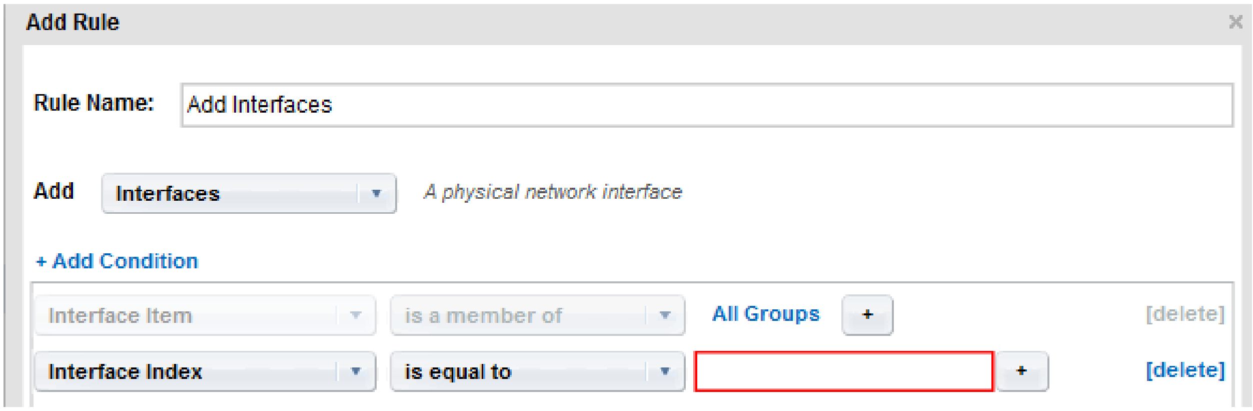
7. Supply a name for the rule in the Rule Name field.

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

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

9. Click Add Condition.

   A row of drop-down lists and fields appears.



Add Rule

Rule Name: Add Interfaces

Add: Interfaces — *A physical network interface*

Interface Item | is a member of | All Groups

Interface Index | is equal to |

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

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

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

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

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

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

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

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

    An 'OR' field appears.

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

    Three more drop-down lists appear.

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

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

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

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

    Each item type requires its own rule.

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

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

Add Managed Items to a Group Manually

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

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

Follow these steps:

1. Navigate to the Manage Groups page.

   The current groups appear in a tree structure.

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

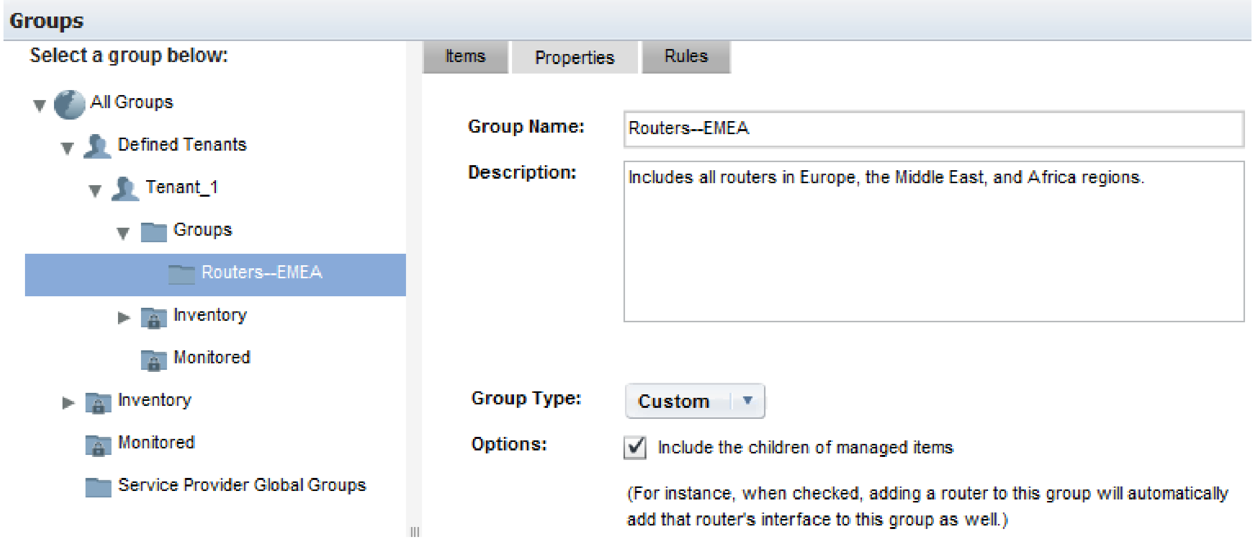
2. Expand the nodes in the Groups tree to locate and select the group to which you want to add managed items.

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

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

3. Click the Properties tab in the right pane.

   The Properties page opens.



Group Name: Routers--EMEA

Description: Includes all routers in Europe, the Middle East, and Africa regions.

Group Type: Custom

Options: ☑ Include the children of managed items

(For instance, when checked, adding a router to this group will automatically add that router's interface to this group as well.)

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

   Include the children of managed items

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

5. Click Save.

6. Click the Items tab.

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

7. Click Add Item Type.

   The Add Items dialog opens.

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

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

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

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

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

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

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

11. Click Add Items.

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

12. Click Close when you have finished adding items.

    The Add Items dialog closes.

    The Items tab shows the items that you have added.

Assign Permissions to Users

Individual CA Performance Center operators require data access permissions to monitor data from MSP customers. CA Performance Center access permissions are based on groups. You can assign access permissions according to your plan for custom groups (see page 40).

To assign permissions, edit CA Performance Center user accounts. Your goal is to make sure that all operators see only the data they require to do their job.

Follow these steps:

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

   The Manage Users page opens.

3. Select a user account that you want to change, and click Edit.

   The Add User wizard opens.

4. Click the Permission Groups button.

   The wizard advances to the Permission Groups page.

5. 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 the right arrow button to add it to Selected Groups on the right.
   - Repeat as necessary.

   The selected permission groups appear in the Selected Groups pane.

6. Select a group from the 'Default Group' drop-down list.

   When the user logs in, data from the default group appears in dashboards by default.

7. Click Save.

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

Custom groups have been created and assigned as permissions to IT staff. When staff members log in to CA Performance Center, they can now view data from the MSP customer systems assigned to them.

Glossary

domain

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

global 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.

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.

role

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

SNMP profiles

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

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.

Index