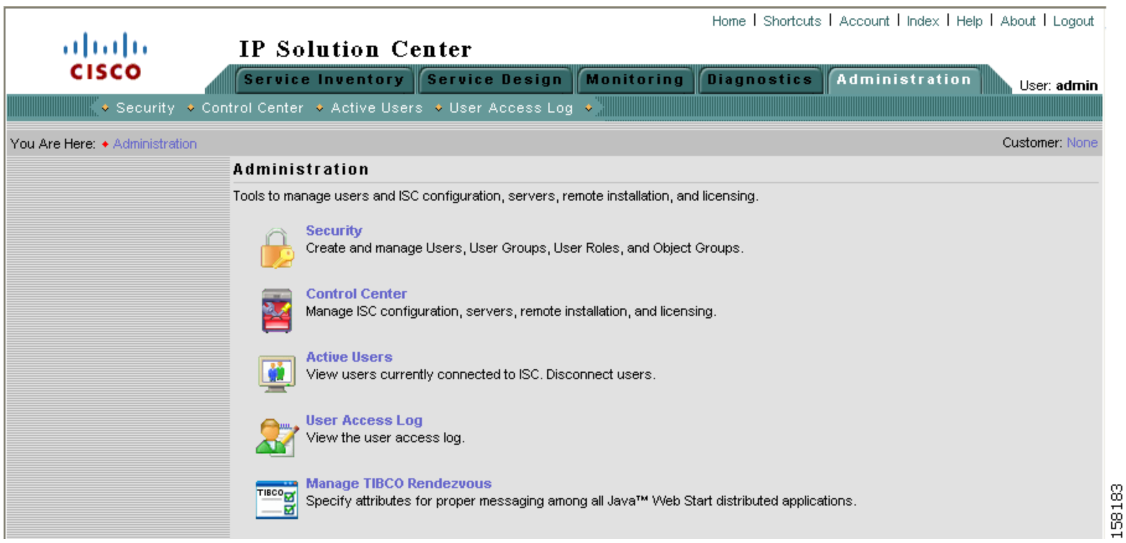
CHAPTER 9

Administration

From the Home window of Cisco IP Solution Center (ISC), which you receive upon logging in, click the **Administration** tab and you receive a window as shown in Figure 9-1, "Administration Selections."

Figure 9-1 Administration Selections



Then you can choose the following selections:

- **Security, page 9-1** Create and manage Users, User Groups, User Roles, and Object Groups
- **Control Center, page 9-21** Manage ISC configuration, servers, and licensing
- **Active Users, page 9-30** View users currently connected to ISC. Disconnect users.
- **User Access Log, page 9-31** View the user access log.
- **Manage TIBCO Rendezvous, page 9-33** Specify attributes for proper messaging among all Java™ Web Start distributed applications.

Security

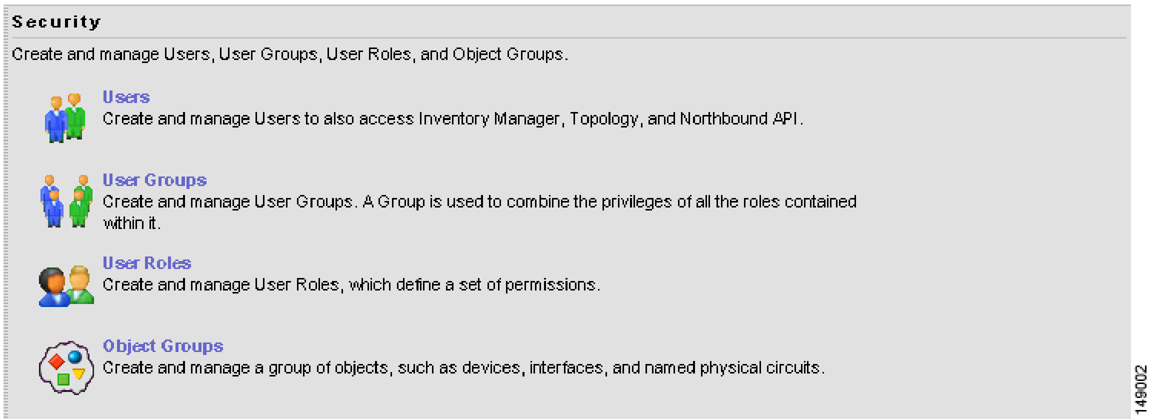
This section describes how system administrators create, edit, and delete users, user groups, user roles, and object groups and how privileges are assigned to these entities.

The security features are only accessible to the user **admin** or users with the following roles:

- **SysAdminRole** gives access to all the ISC tools. This is similar to “root” in a UNIX system.
- **UserAdminRole** gives access to only the user management tools in **Administration** > **Security**.

Choose **Administration** > **Security** to access the user management tools. The window shown in Figure 9-2, “Security Window,” appears.

Figure 9-2 Security Window



From the Security window, choose the following:

- Users, page 9-2 to manage users
- User Groups, page 9-7 to manage user groups
- User Roles, page 9-9 to manage user roles
- Object Groups, page 9-15 to manage object groups.

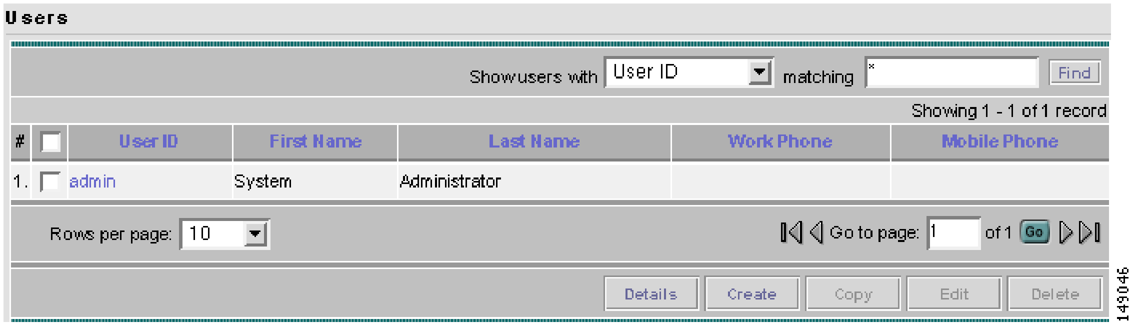
For an example of how to use the Users, User Groups, User Roles, and Object Groups, see the “User Roles Design Example” section on page 9-18.

Users

Choose **Administration > Security > Users** and follow these steps:

Step 1 The window in Figure 9-3, “Users Window,” appears.

Figure 9-3 Users Window



Step 2 The explanations of the buttons are given as follows:

- Details, page 9-3 View a User Detail Report
- Create, page 9-3 Create a new user
- Copy, page 9-6 Make a copy of an existing user and make changes to create a new user
- Edit, page 9-6 Edit selected user
- Delete, page 9-6 Delete selected user(s).

Details

When you click the **Details** button, located at the bottom of Figure 9-3, you receive the following columns of information: **User ID**; **User Group** that a user belongs to; **Role** that a user occupies; **Resource Privilege** permissions that a user has for each role occupied; **Object Group** that a user role is associated with; **Customer View** that a user's role is limited to; **Provider View** that a user's role is limited to.

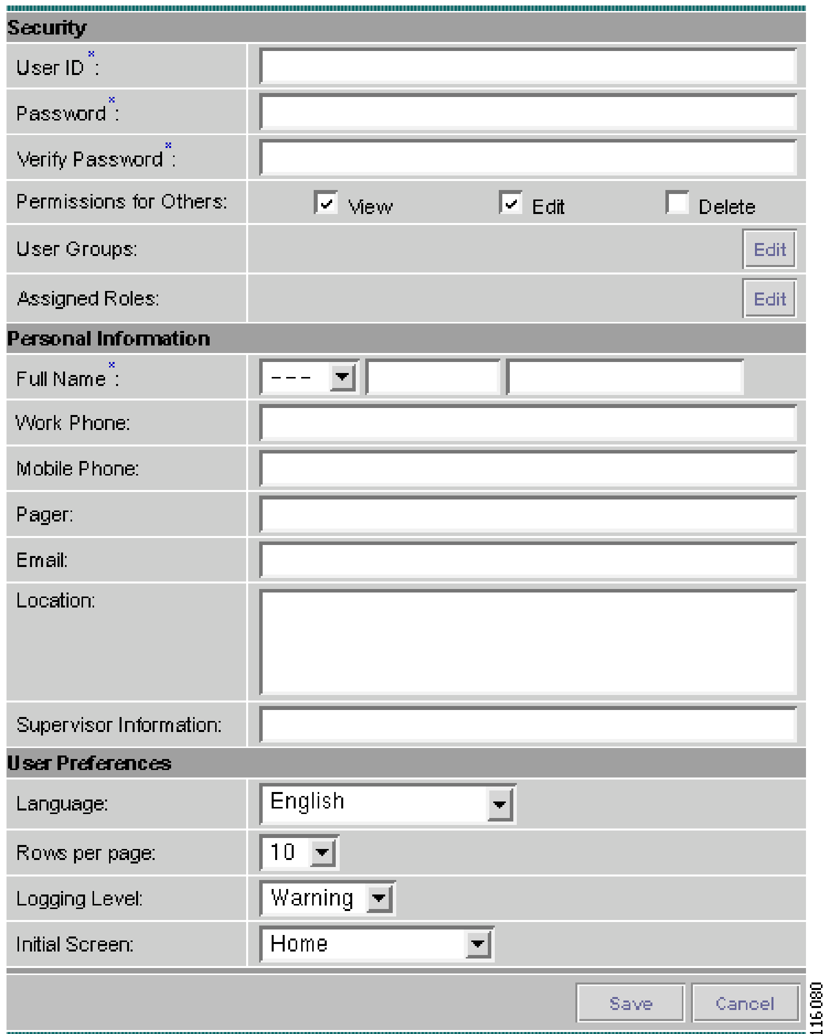
Create

When you click the **Create** button, located at the bottom of Figure 9-3, a user with the required privileges can create a new user. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Click the **Create** button and the window shown in Figure 9-4, "Create/Copy/Edit Users Window," appears.

Figure 9-4 Create/Copy/Edit Users Window



Step 3 Enter information in the **Security** section, as follows:

- **User ID** (required) Enter a User ID for this new user.
- **Password** (required) New password to replace any existing password:
  - ISC requires a non-blank password.
  - ISC passwords must be a minimum of five characters and no practical maximum length.
  - ISC does not employ any password restrictions or complexity rules; use good judgment in determining passwords.
  - ISC passwords are encrypted when stored in the repository.
  - ISC passwords do not expire.
  - ISC monitors inactivity and auto-logoff per the settings defined in the Dynamic Component Properties Library (DCPL) properties for **repository/rbac**, see Appendix C, “Property Settings.”
- **Verify Password** (required) Confirm by re-entering the selected password.

- **Permission for Others** Check each of the associated check boxes for the permission that the user (to be created) wants to give to other users. The user who creates the object is the owner of the objects. The creator can allow or disallow other users to **View**, **Edit**, and/or **Delete** the objects owned by the creator by defining permissions. This is the last line of defense. For UserA to delete an object X that UserB created, UserA must first have Delete permission for object X, then UserB's settings for permissions for others is checked, to finally decide whether UserA can delete object X. Permission for others can be enabled or disabled by setting the property: **repository.rbac.checkCreatorPermissionEnabled**. After you make a change, you must restart the WatchDog by entering **stopwd** followed by **startwd**. For more WatchDog details, see Chapter 2, "WatchDog Commands".
- **User Groups** Click **Edit** and you receive a list of the groups. Add this user to a user group(s). The user inherits all the roles assigned to the group(s). You can filter this list. From the selected groups, check the check box next to each group to which you want to add this user. Then click **OK**. You can repeat this procedure if you want to change your selection.

  A user's group membership can also be changed in the group editor (see the "Edit" section on page 9-8).
- **Assigned Roles** Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role to which you want to assign this user. Then click **OK**. You can repeat this procedure if you want to change your selection.

  The user inherits all the privileges from the groups in which it participates and from the roles assigned to it. That is, the permissions received by the user is an OR result of the permissions in each role.

Step 4 Enter information in the **Personal Information** section, as follows:

- **Full Name** (required) Click the drop-down list and select a title; enter the first name; and then enter the last name.
- **Work Phone** (optional) Enter the work phone number.
- **Mobile Phone** (optional) Enter the user's cell phone or mobile phone number.
- **Pager** (optional) Enter the user's pager number.
- **Email** (optional) Enter the user's e-mail address.
- **Location** (optional) Enter the user's location.
- **Supervisor Information** (optional) Enter information about the supervisor.

Step 5 Enter information in the User Preferences section, as follows:

- **Language** (optional) Click the drop-down list to select a language (at this time only English is supported).
- **Rows per page** (optional) This defines the number of rows per page for object listing. The default is **10**. The choices are: **5**, **10**, **20**, **30**, **40**, **50**, **100**, **500**, **1000**, and **2500**.
- **Logging Level** (optional) The default is **Warning**. The choices are: **Off**, **Severe**, **Warning**, **Config**, **Info**, **Fine**, **Finer**, **Finest**, and **All** (see all levels of logs). This defines the logging level for viewing logging events. The list progresses from the least number of messages to the most number of messages.
- Initial Screen (optional) The default is **Home**. The choices are: **Home**, **Service Inventory**, **Service Design**, **Monitoring**, **Administration**, **Site Index**, and **Diagnostics**. This is a way to specify the first window you will see after logging in.

Step 6 Click **Save**. Figure 9-3 reappears with the new user listed.

Copy

The **Copy** button, located at the bottom of Figure 9-3, provides a convenient way to create a new User by copying the information for an existing User including User Groups, Assigned Roles, and User Preferences. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Check one check box for the existing User you want to copy and edit to create a new User.

Step 3 Click the **Copy** button and the window shown in Figure 9-4, "Create/Copy/Edit Users Window," appears.

Step 4 Required entries are a **User ID**, **Password**, **Verify Password**, and **Full Name**.

Step 5 Make all the other changes you want by following the instructions in the "Create" section on page 9-3.

Step 6 Click **Save** and you will return to Figure 9-3. The newly created **User** is added to the list and a Status Succeeded message appears in green.

Edit

The **Edit** button, located at the bottom of Figure 9-3, allows a user with the required privileges to edit user-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Check the check box for the row of the user you want to edit.

Step 3 Click the **Edit** button and a window as shown in Figure 9-4, "Create/Copy/Edit Users Window," appears.

Note To change your password without the SysAdmin or UserAdmin privileges, click the **Account** tab on the top of the Home page. This allows the user to edit the user profile, including changing the password.

Step 4 Enter the desired information for the user profile, as specified in the "Create" section on page 9-3.

Step 5 Click **Save**. Figure 9-3 reappears with the edited user listed.

Delete

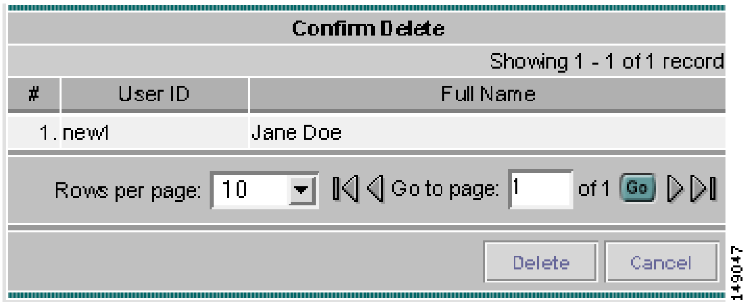
The **Delete** button, located at the bottom of Figure 9-3, allows a user with the required privileges to delete user-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Users**.

Step 2 Check the check box(es) for the row(s) of the user(s) you want to delete.

Step 3 Click the **Delete** button and a window as shown in Figure 9-5, "Users Confirm Delete" appears.

Figure 9-5 Users Confirm Delete



Step 4 Click **Delete** to continue with the process of deleting information for the specified user(s). Otherwise click **Cancel**.

Step 5 Figure 9-3, "Users Window," reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

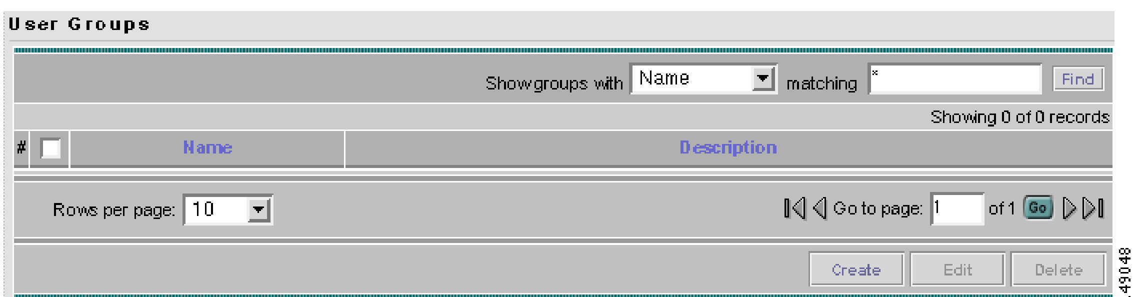
User Groups

A user group is a logical grouping of users with common privileges. The **User Groups** feature is used to create, edit, or delete user groups.

To access the User Groups window, choose **Administration** > **Security** > **User Groups** and follow these steps:

Step 1 The window in Figure 9-6, "User Groups Window" appears.

Figure 9-6 User Groups Window



Step 2 The explanations of the remainder of the buttons is given as follows:

- Create, page 9-8 Create a new user group
- Edit, page 9-8 Edit selected user group
- Delete, page 9-9 Delete selected user group(s)

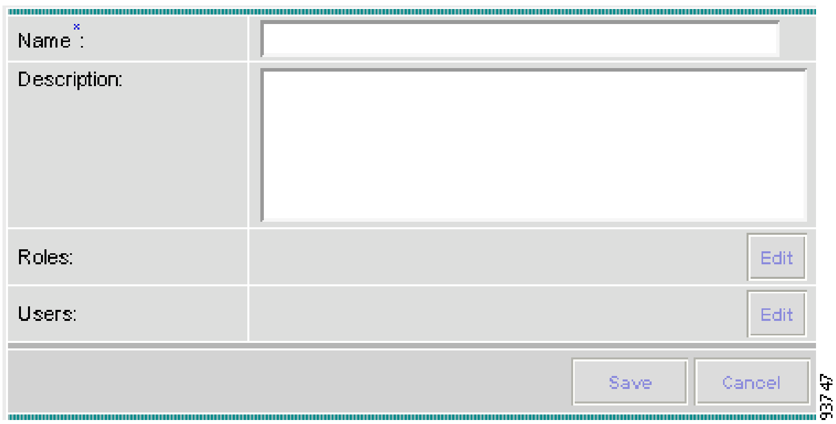
Create

The **Create** button, located at the bottom of Figure 9-6, allows a user with the required privileges to create a user group. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Groups**.

Step 2 Click the **Create** button and the window shown in Figure 9-7, "Create/Edit User Groups Window," appears.

Figure 9-7 Create/Edit User Groups Window



Step 3 Enter information for the user group profile, as follows:

- **Name** (required) Enter a name for the new user group.
- **Description** (optional) Enter a description of this new user group.
- **Roles** This allows you to assign roles to this user group. Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.
- **Users** This allows you to add users to this user group. Click **Edit** and you receive a list of the users. You can filter this list. From the selected users, check the check box next to each user you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 Click **Save**. Figure 9-6 reappears with the new user group listed.

Edit

The **Edit** button, located at the bottom of Figure 9-6, allows a user with the required privileges to edit user group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Groups**.

Step 2 Check the check box for the row of the user group you want to edit.

Step 3 Click the **Edit** button and a window as shown in Figure 9-7, "Create/Edit User Groups Window," appears.

Step 4 Enter the desired information for the user group profile, as specified in Step 3 of the "Create" section on page 9-8.

Step 5 Click **Save.** Figure 9-6 reappears with the edited user group list.

Delete

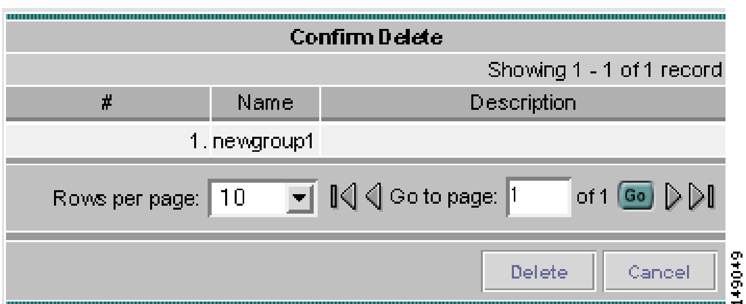
The **Delete** button, located at the bottom of Figure 9-6, allows a user with the required privileges to delete user group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Groups**.

Step 2 Check the check box(es) for the row(s) of the user group(s) you want to delete.

Step 3 Click the **Delete** button and a window as shown in Figure 9-8, "User Groups Confirm Delete," appears.

Figure 9-8 User Groups Confirm Delete



Step 4 Click **Delete** to continue the process of deleting information for the specified user group(s). Otherwise click **Cancel**.

Step 5 Figure 9-6, "User Groups Window," reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Roles

A user role is a predefined or a user-specified role defining a set of permissions. The **User Roles** feature is used to create, edit, or delete user roles.

To better understand the way roles are managed, certain specific characteristics of roles are defined as follows:

- **Parent Role** All permission of the parent roles are inherited by the role that is being created or edited (child role). A child role always has the same or more privileges than its parent role.

- **Customer** If a role is associated with a customer, a user of this role does not have access to the objects associated with other customers. Object types that are constrained by customer view are: Persistent Task, Customer Site, VPN, CPE, SR, Policy, Service Order, and resource pools that are associated with a Customer, Customer Site, or VPN.
- **Provider** If a role is associated with a provider, a user of this role does not have access to the objects associated with other providers. Object types that are constrained by provider view are: Persistent Task, Access Domain, Region, PE, Policy, and some resource pools that are associated with a provider, Access Domain, Region, or PE.

Customer view and provider view within a role have no affect on those objects that do not belong to either a customer or a provider. Those object types are: task, probe, workflow, device, ISC host, and template.

Permission operation types in a Role editor, namely View, Create, Edit, and Delete mean View, Create, Modify, and Delete a database object. For example, SR modification (or subsumption) is viewed as Role Based Access Control (RBAC) Creation. SR purge is viewed as RBAC Delete.

A Role can be enabled to be associated with Object Group(s). When Object Group association is enabled, a Role can no longer be associated with a Customer or a Provider, and it cannot have a Parent Role. Resources are limited to PE, CPE, and Named Physical Circuit only. PE and CPE permission implies Device Permission.

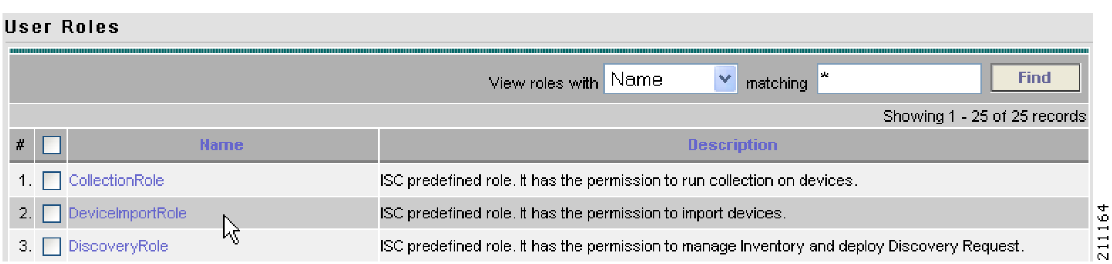
Note A global policy, the one that is not associated with any customer or provider, is accessible by both customer-view roles and provider-view roles.

Separate provider-view from customer-view roles when defining a role. When a role is associated with a provider, choose only the resources for which an access scope can be constrained by a provider view. Do the same for a customer-view role.

To access the User Roles window, choose **Administration** > **Security** > **User Roles** and follow these steps:

Step 1 The window in Figure 9-9, "User Roles Window," appears.

Figure 9-9 User Roles Window



The predefined roles are provided with associated permissions that cannot be edited or deleted. They are intended to cover most of the needed use cases to facilitate a rapid assignment of roles to users and groups with minimum manual configuration. They can also be used as examples to create new roles.

Step 2 The explanations of the buttons is as follows:

- Create, page 9-11 Create a new user role
- Copy, page 9-13 Copy selected user role

- Edit, page 9-14 Edit selected user role
- Delete, page 9-14 Delete selected user role(s)

Create

The **Create** button, located at the bottom of Figure 9-9, allows a user with the required privileges to create a new user role. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Roles**.

Step 2 Click the **Create** button and a window comprised of Figure 9-10, "Create/Copy/Edit User Roles Window (Top)," and Figure 9-11, "Create/Copy/Edit User Roles Window (Bottom)," appears.

Figure 9-10 Create/Copy/Edit User Roles Window (Top)

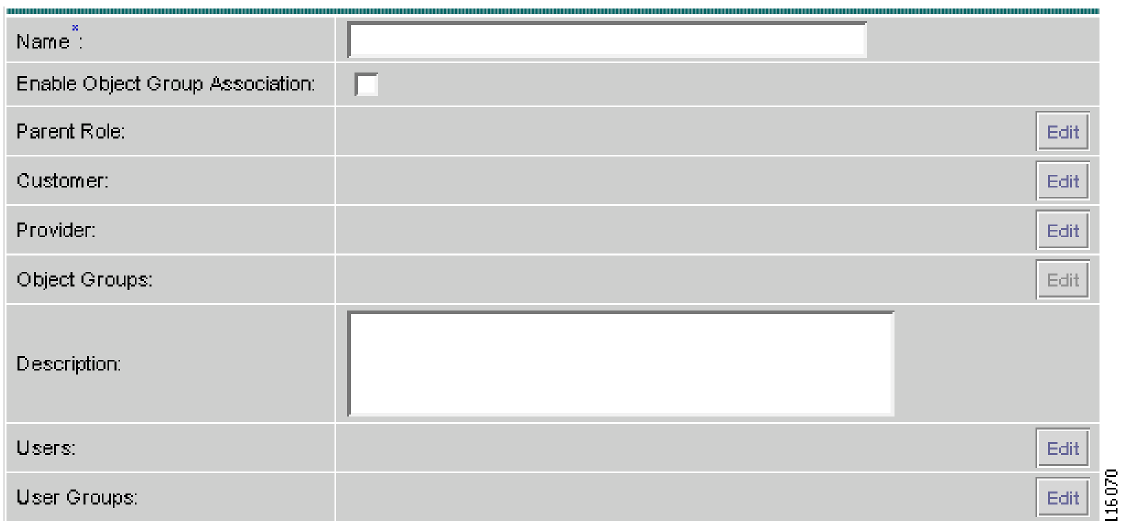
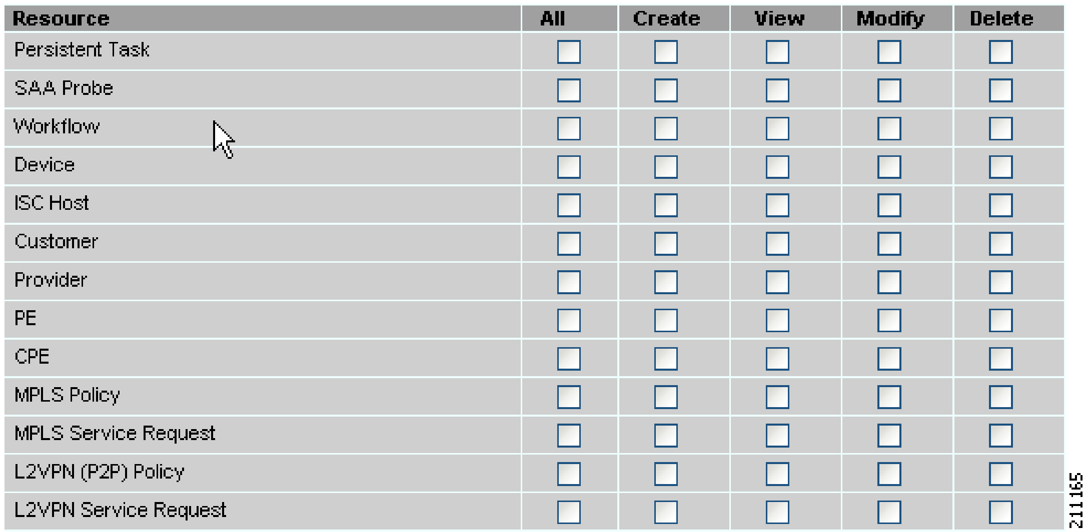


Figure 9-11 Create/Copy/Edit User Roles Window (Bottom)



Step 3 Enter the following information in Figure 9-10:

- **Name** (required) Enter the name of this new user role.
- **Enable Object Group Association** The default is that this check box is unchecked. In this case, **Parent Role**, **Customer**, and **Provider** are enabled and **Object Groups** is not enabled. A complete list of resources appears, as shown in the example in Figure 9-9. If you check this check box, **Parent Role**, **Customer**, and **Provider** are not enabled and **Object Groups** is enabled. A window, as shown in Figure 9-11, is reduced to just **PE**, **CPE**, and **Named Physical Circuit**.
- **Parent Role** (optional) Click **Edit** and a list of the existing roles appears, similar to Figure 9-9, from which you can click the radio button for the parent role you choose. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no parent selection.
- **Customer** (optional) Click **Edit** and a list of the existing customers appears. You can filter this list. From the selected customers, click the radio button for the customer you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no customer selection.

Note A customer can only be associated with a logical device, such as **CPE** and **PE**. This is not possible with a physical device, such as **device**.

- **Provider** (optional) Click **Edit** and a list of the existing providers appears. You can filter this list. From the selected providers, click the radio button for the provider you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no provider selection.
- **Object Groups** (optional) Click **Edit** and a list of the existing object groups appears. You can filter this list. From the selected object groups, check the check box(es) for the object group(s) you want to associate with this User Role. Then click **OK**. You can repeat this procedure if you want to change your selection. Deselect the **Enable Object Group Association** button is you want no object group selection.
- **Description** (optional) Enter the descriptive information about permissions in this field, as shown in the Description column of Figure 9-9.

- **Users** (optional) Click **Edit** and a list of the existing users appears. You can filter this list. From the selected users, check the check box(es) for the user(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Note A user who is associated with a specific role cannot see objects associated with other customers or with other providers.

- **User Groups** (optional) Click **Edit** and a list of the existing user groups appears. You can filter this list. From the selected user groups, check the check box(es) for the user group(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 In Figure 9-11, click any combination of the following permissions: **Create**; **View**; **Modify**; **Delete**. If you want all the permissions, click **All**.

Note **ISC Host** refers to **Administration > Control Center**. Here, you can view host details, perform configuration tasks, start and stop servers, activate a watchdog, and so on.

Note **SAA Probe** is intended for management of SLA under **Monitoring > SLA**. Any user who wants to generate SLA reports *must* have **View** permission on **ISC Host** in addition to **View** permission on **SAA Probe**.

Note The **Workflow** object is currently not used.

Step 5 Click **Save**. Figure 9-9 reappears with the new user role listed.

Copy

The **Copy** button, located at the bottom of Figure 9-9, provides a convenient way to copy the information from an existing User Role and edit it to create a new User Role. Follow these steps:

Note All fields in the existing role are copied to the new role, even including Users and User Groups. You should edit the new role *carefully* to reflect your intention.

Step 1 Choose **Administration** > **Security** > **User Roles**.

Step 2 Check one check box for the existing User Role you want to copy and edit to create a new User Role.

Step 3 Click the **Copy** button and the window comprised of Figure 9-10, "Create/Copy/Edit User Roles Window (Top)," and Figure 9-11, "Create/Copy/Edit User Roles Window (Bottom)" appears.

Step 4 The required entry is a **Name**. A default name is given, **Copy of** and the name of the original User Role. You cannot duplicate a **Name**.

Step 5 Make all the other changes you want by following the instructions in the "Create" section on page 9-11.

Step 6 Click **Save** and you will return to Figure 9-9. The newly created **User** is added to the list and a Status Succeeded message appears in green.

Edit

The **Edit** button, located at the bottom of Figure 9-9, allows a user with the required privileges to edit user role-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Roles**.

Step 2 Check the check box for the row of the user role you want to edit.

Step 3 Click the **Edit** button and a window appears combining Figure 9-10 and Figure 9-11 for this user role.

Step 4 Enter the desired information for the user role profile, as specified in Step 3 and Step 4 of the "Create" section on page 9-11.

Step 5 Click **Save**. Figure 9-9 reappears with the edited user roles listed.

Delete

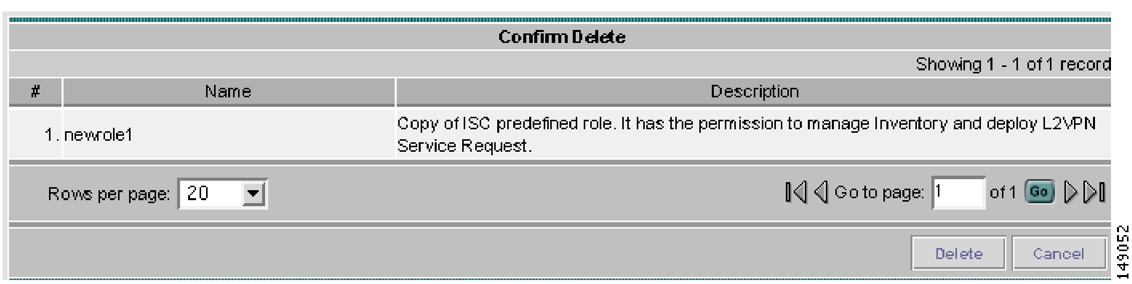
The **Delete** button, located at the bottom of Figure 9-9, allows a user with the required privileges to delete user role-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **User Roles**.

Step 2 Check the check box(es) for the row(s) of the user role(s) you want to delete.

Step 3 Click the **Delete** button and a window as shown in Figure 9-12, "User Roles Confirm Delete," appears.

Figure 9-12 User Roles Confirm Delete



Step 4 Click **Delete** to continue with the process of deleting information for the specified user role(s). Otherwise click **Cancel**.

Step 5 Figure 9-9, "User Roles Window," reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.

Object Groups

An Object Group is a named aggregate entity comprised of a set of objects. The object types can be PE, CE, Named Physical Circuit (NPC), and interfaces of PEs or CEs. An Object Group provides instance level of access granularity for users.

An Object Group can be associated with different roles. A role can be associated with an Object Group or it can be associated with a grouping of Customer and Provider, but it cannot be associated with both of these. The association with a grouping of Customer and Provider is either with Customer(s), with Provider(s), or with Customer(s) and Provider(s). When a role is associated with Object Group(s), you can only define permissions for PE, CE, and NPC. Permissions on interfaces is implied PEs or CEs, that is, PE Create or CE Create implies Interface Create. PE or CE Edit implies Interface Create, Edit, or Delete. CE or PE Delete implies Interface Delete.

When instance level of access is desired for PE, CE, NPC, or interface of PEs and CEs, you can usually define a role associated with Object Group(s) that contains a collection of PEs and CEs you are limited to operate. Then define other roles to include permissions on other types of objects. See the "User Roles Design Example" section on page 9-18.

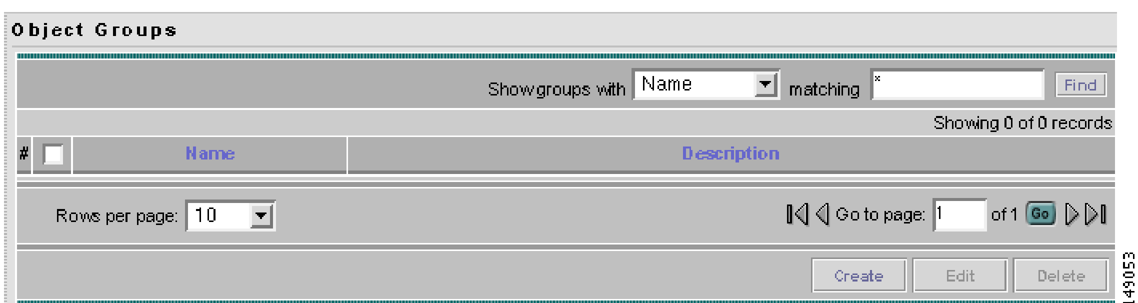
If an Object Group contains PEs (or CEs) only, with no explicit interface as a group member, you can access all interfaces of grouped PEs or CEs. If an Object Group contains any explicit interface as group members, every single interface that you want to access you must manually choose to include as group members.

Note Permissions are the union of all roles that you occupy. If your intention is to limit access to a scope of devices or Named Physical Circuits (NPCs), define a role to be associated with Object Group(s), Device, CE, PE, and NPC.

To access the Object Groups window, choose **Administration** > **Security** > **Object Groups** and follow these steps:

Step 1 The window in Figure 9-13, "Object Groups Window," appears.

Figure 9-13 Object Groups Window



Step 2 The explanations of the buttons is as follows:

- Create, page 9-11 Create a new object group
- Edit, page 9-14 Edit a selected object group
- Delete, page 9-14 Delete selected object group(s)

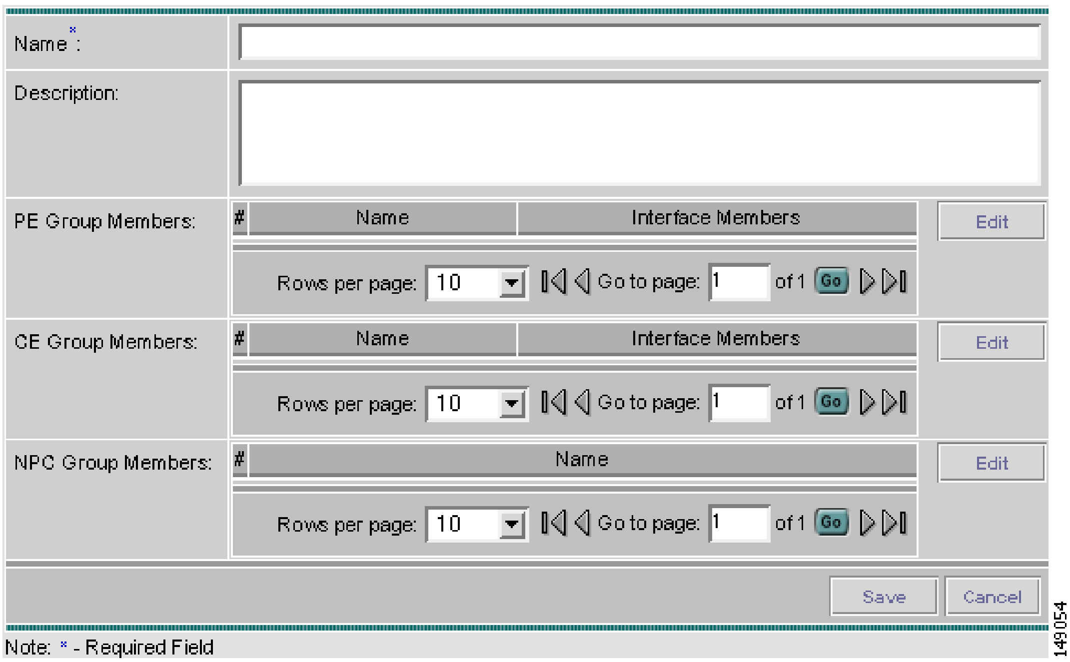
Create

The **Create** button, located at the bottom of Figure 9-13, allows a user with the required privileges to create a new object group. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Object Groups**.

Step 2 Click the **Create** button and the window Figure 9-14, "Create/Edit Object Group Window," appears.

Figure 9-14 Create/Edit Object Group Window



Step 3 Enter the following information in Figure 9-14:

- **Name** (required) Enter the name of this new object group.
- **Description** (optional) Enter a description of this new object group.
- **PE Group Members** (optional) Click **Edit** and a list of the existing PEs appears. You can filter this list. From the selected PEs, check the check box(es) for the PE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column will be empty. All existing interfaces for each of the PE Groups in the **Name** column will default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a PE Group in the **Name** column.You receive a list of all the interfaces for that PE from which you can individually select only the interfaces you want to associate with that PE Group. Then click **OK**. You return to Figure 9-14, "Create/Edit Object Group Window," and the **Name** and selected **Interface Members** for each PE Group Member appear. If no entries exist in the **Interface Members** column for both **PE Group Members** and **CE Group Members**, the default is all existing interfaces for both (if any exist).
- **CE Group Members** (optional) Click **Edit** and a list of the existing CEs appears. You can filter this list. From the selected CEs, check the check box(es) for the CE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column is empty. All existing interfaces for each of the CE Groups in the **Name** column default to be members of the group unless you select only a subset. To limit the interfaces and select

a subset of interfaces, click a CE Group in the **Name** column.You receive a list of all the interfaces for that CE from which you can individually select only the interfaces you want to associate with that CE Group. Then click **OK**. You return to Figure 9-14, "Create/Edit Object Group Window," and the **Name**, and selected **Interface Members** for each CE Group Member appear. If no entries exist in the **Interface Members** column for both **CE Group Members** and **PE Group Members**, the default is all existing interfaces for both (if any exist).

- **NPC Group Members** (optional) Click **Edit** and a list of the existing NPCs appears. You can filter this list. From the selected NPCs, check the check box(es) for the NPC(s) you want to select to own this role. Then click **OK**. You can repeat this procedure if you want to change your selection(s). You return to Figure 9-14, "Create/Edit Object Group Window," and the **Name** for each NPC Group Member appears.

Step 4 Click **Save**. Figure 9-14 reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of Figure 9-14, allows a user with the required privileges to edit object group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Object Groups**.

Step 2 Check the check box for the row of the object group you want to edit.

Step 3 Click the **Edit** button and a window appears as shown in Figure 9-13, with the object group chosen specified in the **Name** field.

Step 4 Enter the desired information for the object group, as specified in Step 3 of the "Create" section on page 9-16.

Step 5 Click **Save**. Figure 9-13 reappears with the edited object groups listed.

Delete

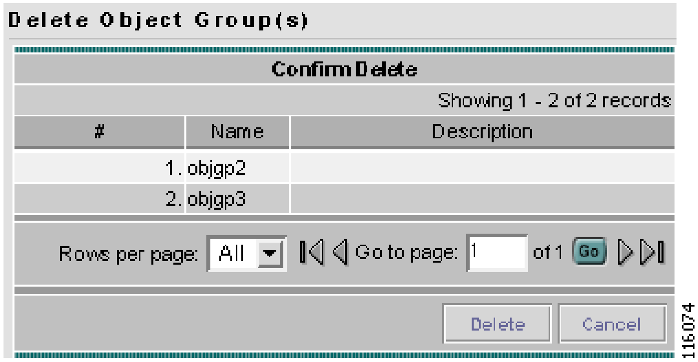
The **Delete** button, located at the bottom of Figure 9-13, allows a user with the required privileges to delete object group-specific information. Follow these steps:

Step 1 Choose **Administration** > **Security** > **Object Groups**.

Step 2 Check the check box(es) for the row(s) of the object group(s) you want to delete.

Step 3 Click the **Delete** button and a window as shown in Figure 9-15, "Delete Object Groups Confirm Delete," appears.

Figure 9-15 Delete Object Groups Confirm Delete



Step 4 Click **Delete** to continue with the process of deleting information for the specified object group(s). Otherwise click **Cancel**.

Step 5 Figure 9-13, "Object Groups Window," reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Roles Design Example

This section gives an example situation, an illustration that shows this setup, and steps on how to setup this design:

- Example, page 9-18
- Illustration of Setup, page 9-19
- Steps to Set Up Example, page 9-20

Example

This section explains an example data center for which the following sections, "Illustration of Setup" section on page 9-19 and "Steps to Set Up Example" section on page 9-20 give an illustration setup and steps, respectively.

Finance Customer XYZ built an MPLS network to connect its branch offices to its data center. Subsidiaries of XYZ are running different parts of the MPLS network. Each subsidiary uses a different BGP AS domain, which results in different Provider Administrative Domains (PADs) inside ISC.

Each subsidiary acts as a Provider and owns therefore its own Devices, like PE and CE devices, and should also own logical attributes inside ISC, like Regions, Sites, Customers, and VPNs. Therefore, the view of the devices for each subsidiary must be separated into PAD views. Thus, Provider A cannot manipulate or view the configuration files for devices of Provider B. Devices are not shared between PADs.

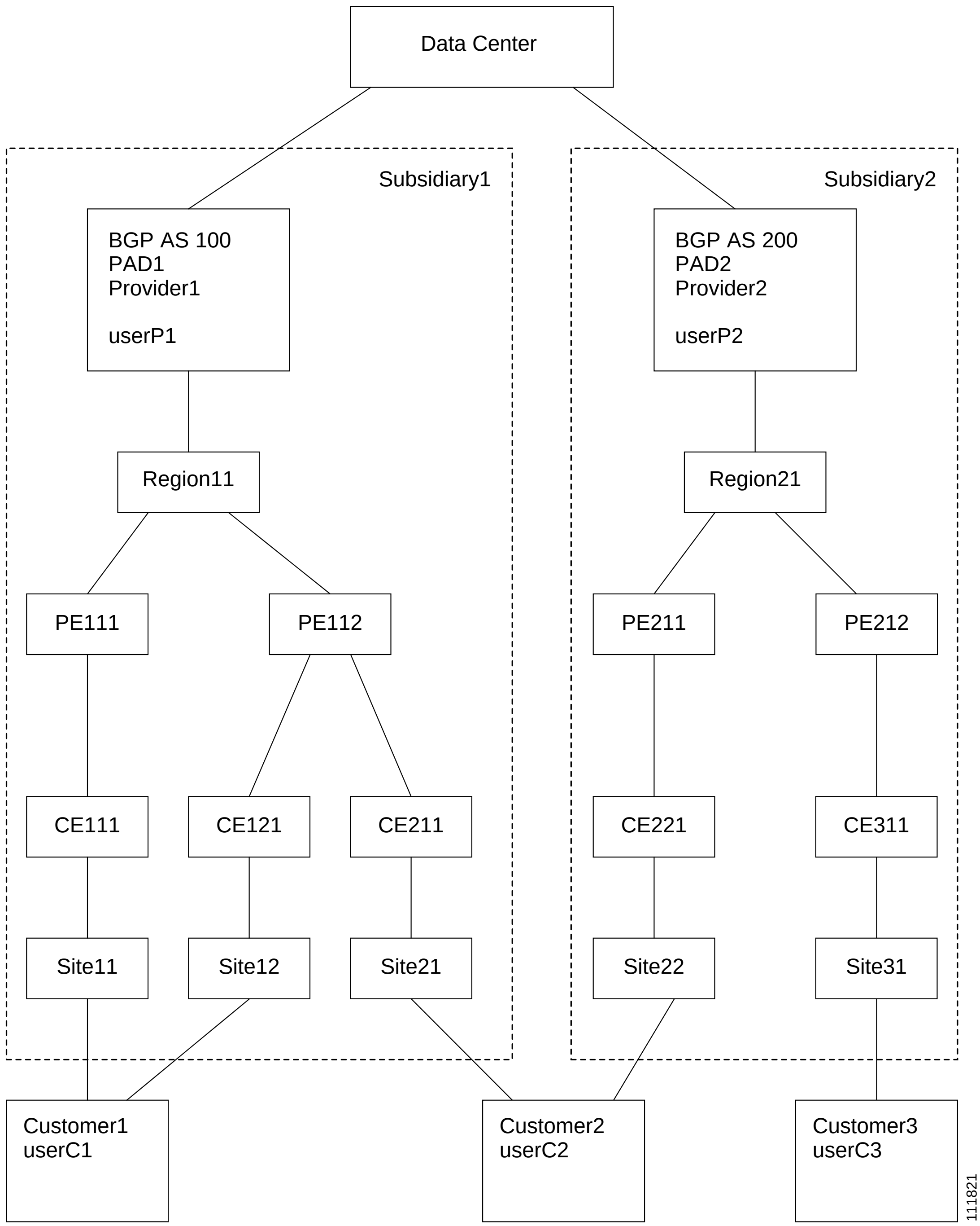
Inside a PAD, there are Customers with sites and VPNs with only local significance. Also, the IP addressing should be defined per PAD.

But there are also Customers that have sites in different PADs. This means that there is a need for Inter-AS VPNs. The Provider who owns the Customer should also have the right to share this Customer with other Providers. In this case, the VPNs and CERCs should be shared between the providers.

Illustration of Setup

Figure 9-16, "Contents in Example," shows the setup described in the "Example" section on page 9-18.

Figure 9-16 Contents in Example



Steps to Set Up Example

This section explains the steps to create the example explained in the "Example" section on page 9-18 and shown in the "Illustration of Setup" section on page 9-19.

Step 1 Create the following Object Groups (see the "Create" section on page 9-16, which is for the section Object Groups):

- P1PEGroup that has members PE111 and PE112
- P2PEGroup that has members PE211 and PE212
- C1CEGroup that has members CE111 and CE121
- C2CEGroup that has members CE211 and CE221
- C3CEGroup that has the member CE311
- C2DeviceGroup that has members PE112, CE211, PE211, and CE221
- C3DeviceGroup that has members PE212 and CE311.

Step 2 Create the following User Roles that are associated with one or more groups created in Step 1 (see the "Create" section on page 9-11, which is for the section User Roles.

- P1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and C2CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
- P2DeviceGroupRole, associated with groups P2PEGroup, C2CEGroup, and C3CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
- C1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
- C2DeviceGroupRole, associated with group C2DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
- C3DeviceGroupRole, associated with group C3DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.

Step 3 Create the following User Roles that have Customer View or Provider View, as explained in the "User Roles" section on page 9-9.

- P1MplsRole, associated with Provider P1, and have permissions on Provider, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- P2MplsRole, associated with Provider P2, and have permissions on Provider, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- C1MplsRole, associated with Customer C1, and have permissions on Customer, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- C2MplsRole, associated with Customer C2, and have permissions on Customer, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- C3MplsRole, associated with Customer C3, and have permissions on Customer, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)

Step 4 Assign the User Roles defined in Step 2 and Step 3 to Users, as explained in the "Users" section on page 9-2.

- User P1 has User Roles: P1DeviceGroupRole, P1MplsRole, C1MplsRole, and C2MplsRole.
- User P2 has User Roles: P2DeviceGroupRole, P2MplsRole, C2MplsRole, and C3MplsRole.
- User C1 has User Roles: C1DeviceGroupRole and C1MplsRole.

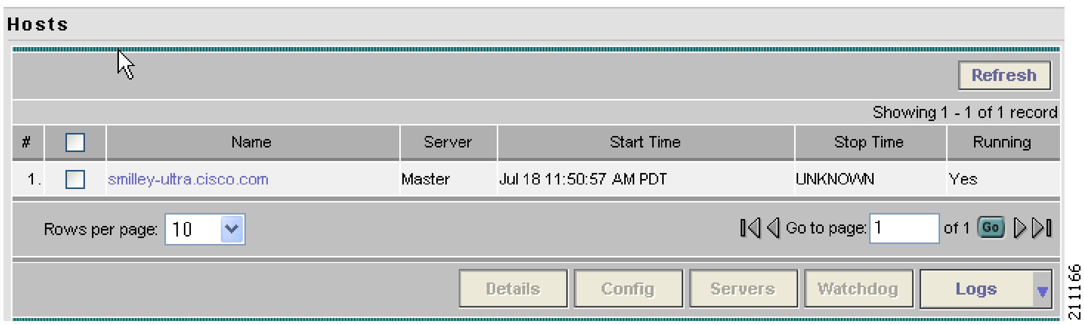
- User C2 has User Roles: C2DeviceGroupRole and C2MplsRole.
- User C3 has User Roles: C3DeviceGroupRole and C3MplsRole.

Control Center

This section explains how to view and change the properties in the Dynamic Component Properties Library (DCPL); how to view status information about a host, servers, the WatchDog, and logs; how to define collection zones; and how to install license keys.

Choose **Administration** > **Control Center** and you go to the default page of **Hosts** in the TOC, as shown in Figure 9-17, "Control Center > Hosts."

Figure 9-17 Control Center > Hosts



From **Administration** > **Control Center**, you have the following three choices in the TOC:

- Hosts, page 9-21 **Hosts** allows you to manage the various servers.
- Collection Zones, page 9-26 **Collection Zones** are the means of associating the Master server with network devices.
- Licensing, page 9-28 **Licensing** is where you install license keys, which is the only way to access services and APIs.

Hosts

Choose **Administration** > **Control Center** > **Hosts**.

A window as shown in Figure 9-17 appears.

Note Only the **Logs** buttons are enabled by default when there is no host selected. When the host is selected by checking the check box, the Logs buttons is disabled and the other buttons are enabled.

Click any of the buttons and proceed as follows:

- Details, page 9-22 Available only when the host system is chosen.
- Config, page 9-23 Available only when the host system is chosen.
- Servers, page 9-24 Available only when the host system is chosen.

- [Watchdog, page 9-25] Available only when the host system is chosen.
- [Logs, page 9-26] Available only when no host system selection is made.

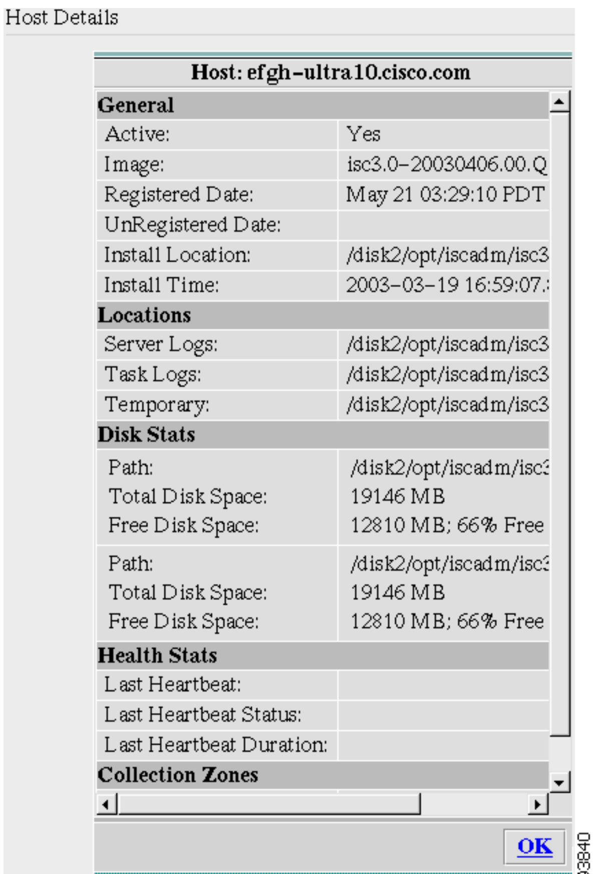
Details

For details about a chosen host, follow these steps:

Step 1 Choose a host by checking the check box to the left of the host name and then click the **Details** button.

Step 2 You receive a window as shown in Figure 9-18, "Host Details." This shows the details about the chosen host.

Figure 9-18 Host Details



Step 3 Click **OK** and you return to Figure 9-17.

Config

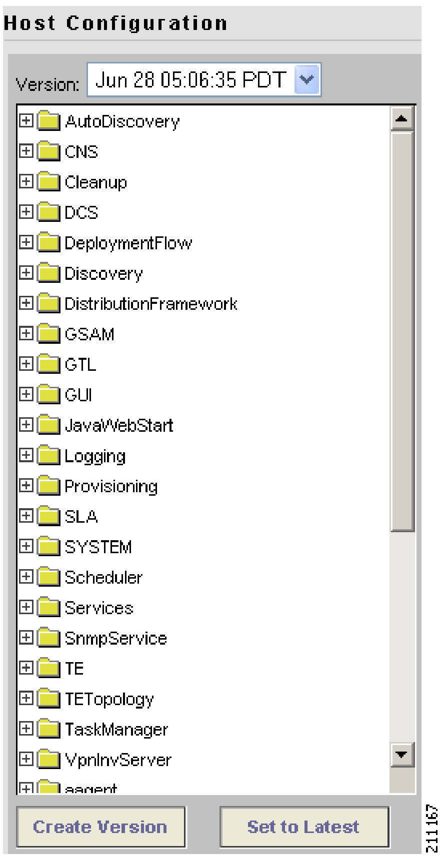
To view or change the Dynamic Component Properties Library (DCPL) properties, which replaces the csm.properties file for VPNSC, follow these steps:

Note csm.properties in VPNSC cannot be migrated to DCPL settings in ISC.

Step 1 From Figure 9-17 on page 9-21, check a check box next to a host name for which you want to know the existing properties and then click the **Config** button.

Step 2 A window as shown in Figure 9-19, "Properties," appears. It is a list of all the folders with all the properties. See Appendix C, "Property Settings" for a list of all the properties with explanations, defaults, and ranges/rules. If you don't know the property name, you can use a key word and do a Find on the pdf version of this appendix.

Figure 9-19 Properties

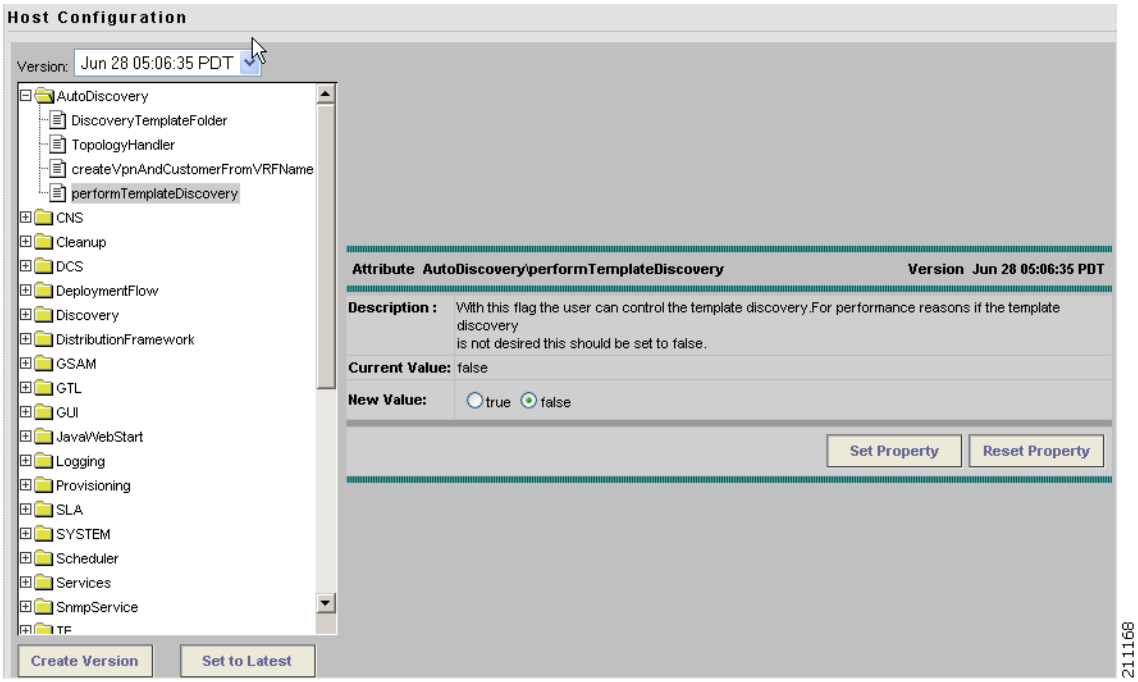


Step 3 Click the + sign to expand each folder. The result could be more subfolders and the final level is the property name.

Step 4 Position the mouse over the folder or property name and you see a description.

Step 5 Click on an entry to get details and instructions on how to change the value, as shown in the example in Figure 9-20, "Properties Detail Example."

Figure 9-20 Properties Detail Example



Step 6 For each property that can be modified, you can modify the value and click **Set Property**. If when making your modifications, you want to return to the previous settings, click **Reset Property**.

Step 7 After making all the changes you choose in each of the specific properties, you can click **Create Version** to create a new version of these properties. This feature gives you the option of saving multiple property sets for future use.

Step 8 To view the values of previous versions of property sets, click the drop-down list in **Version** and select any version you choose.

Step 9 When you click **Set to Latest** after selecting a version in Step 8, this version is dated as the most current.

Step 10 To return, click to the navigation path you want to use next.

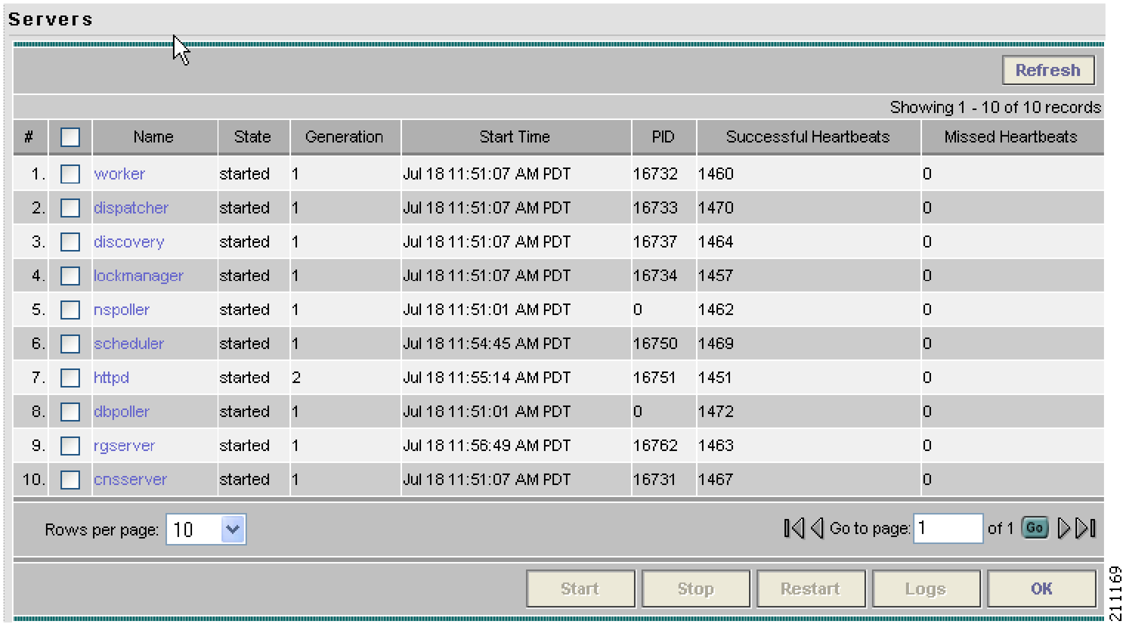
Servers

To view the status information about the servers, follow these steps:

Step 1 From Figure 9-17 on page 9-21, check a check box next to a host name for which you want to know the server statistics and then click the **Servers** button.

Step 2 A window as shown in Figure 9-21, "Servers," appears.

Figure 9-21 Servers



Step 3 Check any one check box next to the server you want to address and you have access to **Start**, **Stop**, **Restart**, and **Logs**. When you click on a specific server name or the Logs button, you get a list of server logs. If you then click on the log name for which you want details, the log viewer appears. You can filter this information in the log viewer. After you complete the task of your choice, you return to Figure 9-21.

Step 4 You can click a different server and click the button for the process of your choice. Or you can unclick the server choice and click **OK**.

Step 5 After you click **OK** in Figure 9-21, you return to Figure 9-17 on page 9-21.

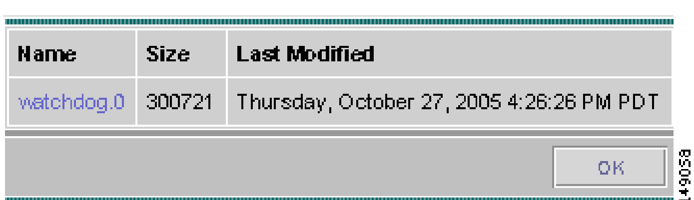
Watchdog

To view the log information about WatchDog, follow these steps:

Step 1 From Figure 9-17 on page 9-21, check a check box next to a host name for which you want to know the WatchDog logs and then click the **Watchdog** button.

Step 2 A window as shown in Figure 9-22, "WatchDog Logs," appears.

Figure 9-22 WatchDog Logs



Step 3 Click on a specific WatchDog log name in the **Name** column to get the contents of that log. You can filter the information in this log. Click **OK** to return to Figure 9-22.

Step 4 You can repeat the process in Step 3 or click **OK** to return to Figure 9-17 on page 9-21.

Logs

To view install and uninstall logs for the Master server, follow these steps:

Step 1 From Figure 9-17 on page 9-21, be sure that no check boxes are checked.

Step 2 Click the **Logs** drop-down list and select **Install** or **Uninstall**.

Step 3 The window that appears is the log of installations or uninstallations, dependent on your selection in Step 2.

Step 4 Click the link in the **Name** column to view the detailed log information.

Step 5 Click **OK** to return to the window in Step 3.

Step 6 Click **OK** again to return to Figure 9-17 on page 9-21.

Collection Zones

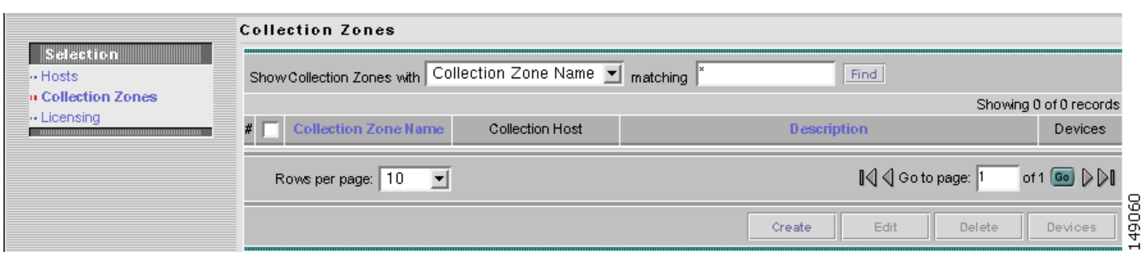
Choose **Administration > Control Center**.

A collection zone is a geographical grouping of devices. Each collection zone is associated with the Master server that collects data from its devices. However, a Master server can service multiple collection zones.

To define collection zones, follow these steps:

Step 1 From the Control Center, choose **Collection Zones** from the TOC in the left column, and a window as shown in Figure 9-23, "Choose Control Center > Collection Zones" appears.

Figure 9-23 Choose Control Center > Collection Zones

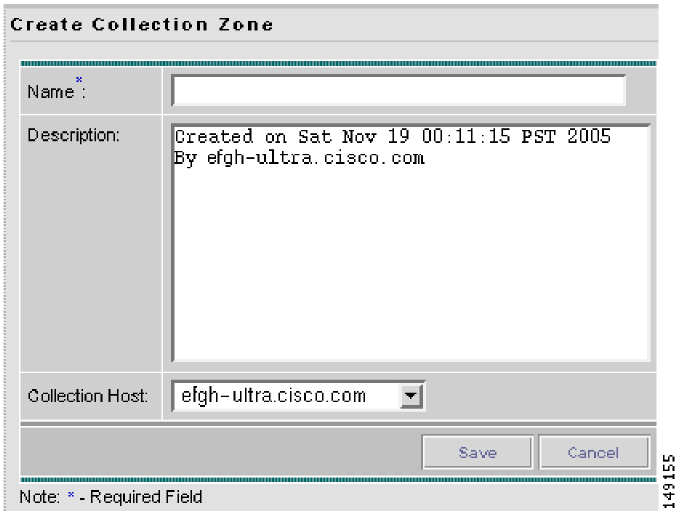


Step 2 To **Create** a collection zone, proceed to Step 3. To **Edit** a collection zone, proceed to Step 6. To **Delete** a collection zone, proceed to Step 8. To display the **Devices**, proceed to Step 11.

Step 3 From Figure 9-23, without checking any check boxes, click the **Create** button.

Step 4 A window as shown in Figure 9-24, "Create Collection Zone," appears.

Figure 9-24 Create Collection Zone



Fill in the following information:

- **Name** (required)
- **Description** (optional) This is automatically filled in with the creation statistics: date, time, and creator. You can overwrite this information, add to it, or delete it altogether.
- **Collection Host** (default host appears) Click the drop-down list if you want to select a different collection host.

Step 5 Click **Save**. Figure 9-23 reappears, the newly created collection zone is added, and a Status appears with a green check mark for **Succeeded**. You can repeat Step 3 to Step 5 to create another collection zone. For **Edit**, proceed to Step 6. For **Delete**, proceed to Step 8. To display the **Devices**, proceed to Step 11.

Step 6 To edit a collection zone, in Figure 9-23, check the check box for the collection zone you want to edit and then click the **Edit** button.

Step 7 A window as shown in Figure 9-24 appears. Follow the instructions in Step 4 and Step 5.

Step 8 To delete a collection zone, in Figure 9-23, check one or more check boxes for the collection zone(s) you want to delete. Then click the **Delete** button.

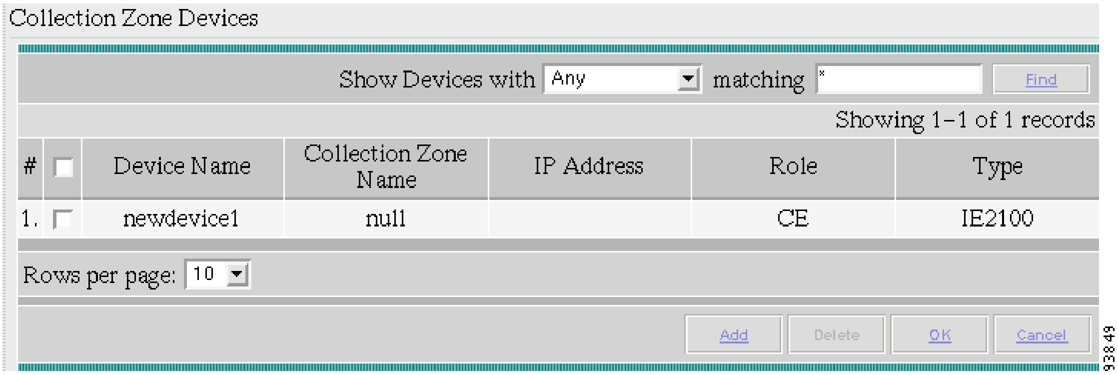
Step 9 A Confirm Delete window appears, to give you a chance to click **Cancel** and not delete, or to click **OK** and delete.

Step 10 Figure 9-23 reappears and the collection zone is removed. You can repeat Step 8 and Step 9 to delete more collection zones, you can proceed to Step 3 to create a collection zone, you can proceed to Step 6 to edit a collection zone, or you can proceed to Step 11 to display and assign devices.

Step 11 To display, add, or delete devices, in Figure 9-23, check a check box for the desired collection zone. Then click the **Devices** button.

Step 12 A window appears as shown in Figure 9-25, "Collection Zone Devices." This window shows the current devices assigned to the selected collection zone.

Figure 9-25 Collection Zone Devices



Step 13 To add a device, click **Add**; to delete devices, select the devices you want to delete from those shown and click **Delete (**this happens automatically with no chance to reconsider, but you can add it back in with another **Add** process**)**; to accept what is listed, click **OK**; or to cancel, click **Cancel**.

Step 14 If you click **Add**, you get a window with all the devices in the database. You can filter the list and from the listed choices you can select one or more devices to add to the selected collection zone. Then click **Select**.

Step 15 Figure 9-25 reappears with the updated device information for the selected collection zone.

Step 16 When Figure 9-25 has all the devices you want, click **OK** and Figure 9-23 reappears with the updated information.

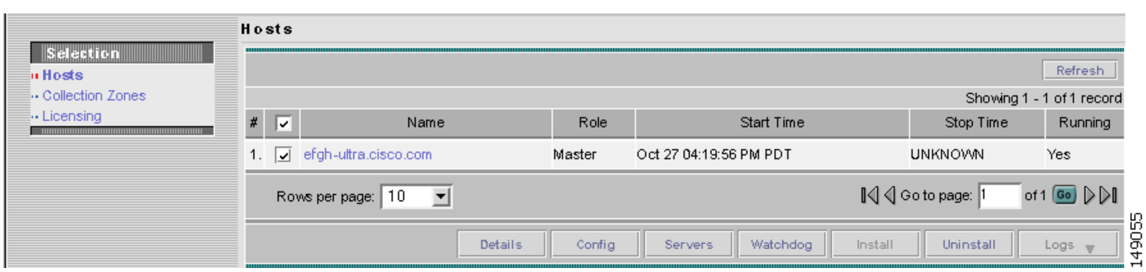
Licensing

Choose **Administration > Control Center**.

To install license keys, follow these steps:

Step 1 From **Control Center**, choose **Licensing** from the TOC in the left column, as shown in Figure 9-26, "Choose Control Center > Licensing."

Figure 9-26 Choose Control Center > Licensing

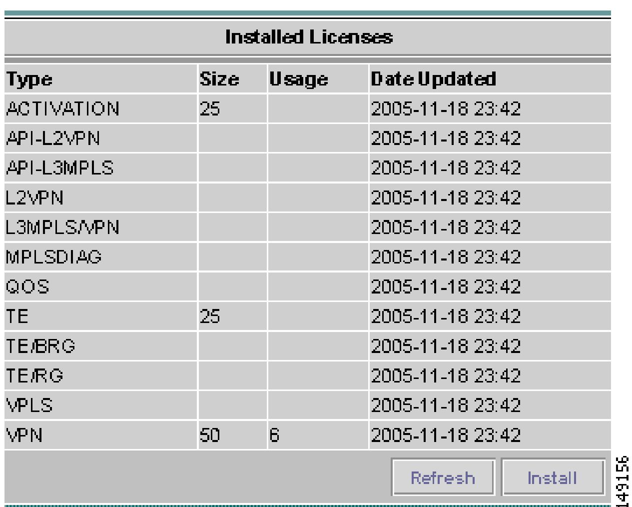


Step 2 From the **Installed Licenses** table, click the **Install** button, as shown in Figure 9-27, "Installed Licenses." The Installed Licenses table explains the current statistics. The columns of information tell the **Type** of license keys you have installed (which can include ACTIVATION, API-L2VPN, API-L3MPLS, L2VPN, L3MPLS/VPN,MPLSDIAG, TE, TE/BRG, TE/RG, VPLS, VPN); the **Size**, which is valid for the **ACTIVATION** (licensed maximum global count of services), **TE** (number of TE-enabled nodes), or the **VPN** (maximum number of VPNs licensed); the **Usage**, which gives the number currently used for the rows; and the **Date Updated**, which reflects the refresh of the license usage (on an hourly basis, by default).

Note When you purchase Traffic Engineering Management (TEM), you automatically receive **TE**, **TE/BRG**, and **TE/RG** licenses. All of these licenses *must* be installed to have access to all the Cisco ISC TEM features, including Planning Tools for protection planning (backup tunnels). The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM (you purchase licenses and upgrade licenses based on a range of nodes); the **TE/RG** license enables primary tunnel placement; and the **TE/BRG** license enables the Fast ReRoute (FRR) protection function.

Note Click **Refresh** to give the most current status.

Figure 9-27 Installed Licenses

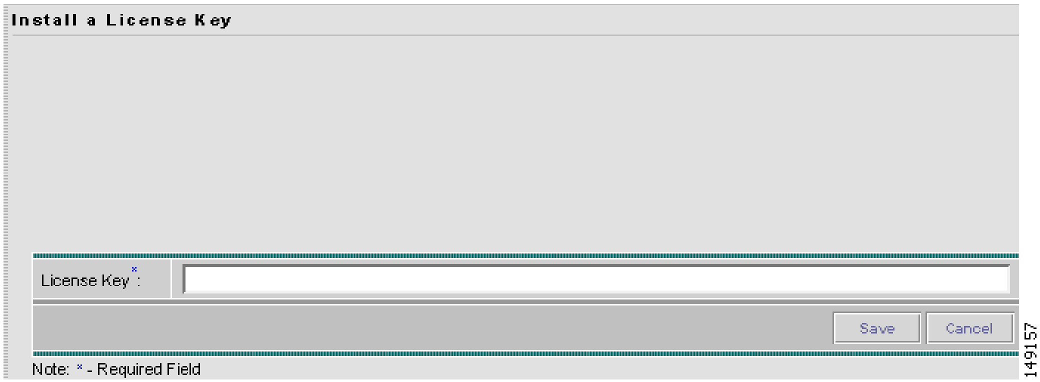


Installed Licenses

Type	Size	Usage	Date Updated
ACTIVATION	25		2005-11-18 23:42
API-L2VPN			2005-11-18 23:42
API-L3MPLS			2005-11-18 23:42
L2VPN			2005-11-18 23:42
L3MPLS/VPN			2005-11-18 23:42
MPLSDIAG			2005-11-18 23:42
QOS			2005-11-18 23:42
TE	25		2005-11-18 23:42
TE/BRG			2005-11-18 23:42
TE/RG			2005-11-18 23:42
VPLS			2005-11-18 23:42
VPN	50	6	2005-11-18 23:42

Step 3 In the resulting window, as shown in Figure 9-28, "Enter License Key," enter a **License Key** that you received on your *Right to Use* paperwork with your product.

Figure 9-28 Enter License Key



Step 4 Click **Save**. Your newly installed license appears in an updated version o f the Installed License table, as shown in Figure 9-27, "Installed Licenses."

Step 5 Repeat Step 2, Step 3, and Step 4 for each of the *Right to Use* documents shipped with your product.

Note When you receive multiple *Right to Use* documents to upgrade either the ACTIVATION License, which activates and sets the maximum global count of the services, or VPN licenses, which activates and set the maximum number of VPNs, be sure to enter the licenses in the correct order. For example, if you are upgrading from 500 to 3000 global count of the services and there are two steps to get there, enter the license to upgrade from 500 to 1500 and then the license key to upgrade from 1500 to 3000.

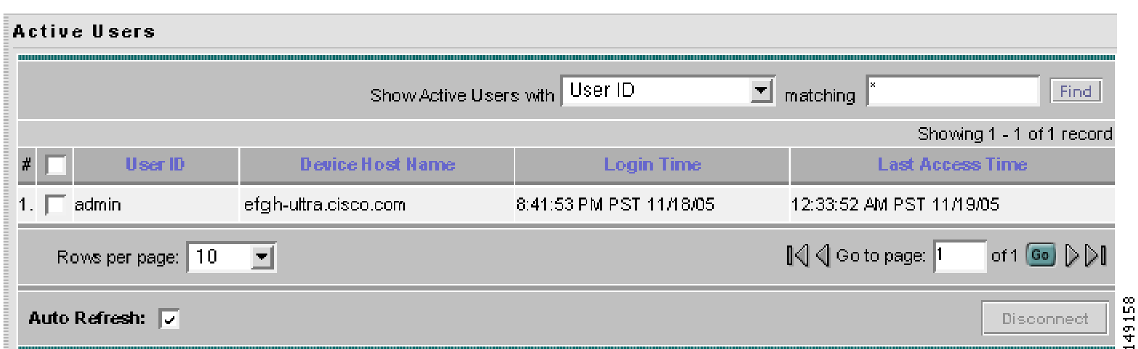
Active Users

This section explains how to communicate with active users.

Choose **Administration** > **Active Users** and follow these steps:

Step 1 After you choose **Administration** > **Active Users**, a window that shows the currently logged users appears, as shown in Figure 9-29, "Active Users."

Figure 9-29 Active Users



Step 2 In Figure 9-29, if you have the privileges of **SysAdmin** or **UserAdmin**, you can disconnect one or more users. Check the check box next to each user you want to disconnect. Then click the **Disconnect** button at the bottom of the window.

Caution The current login sessions for the disconnected users are terminated and their work is lost.

Step 3 To exit this list of all active users, choose another feature from the main product tabs.

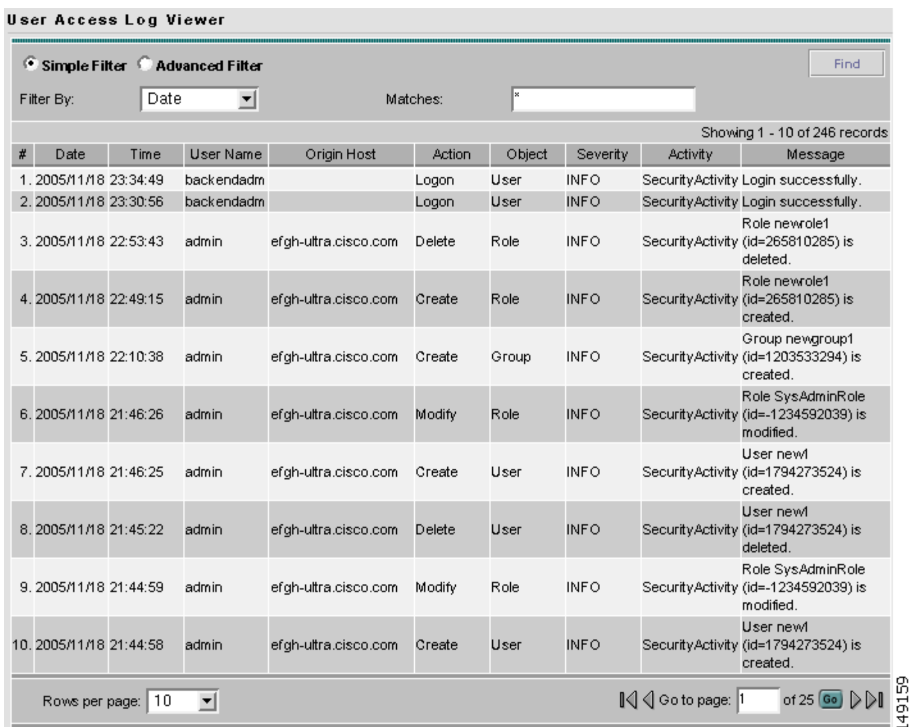
User Access Log

This section shows a detailed report of every activity by every user.

Choose **Administration > User Access Log** and follow these steps:

Step 1 After you choose **Administration > User Access Log**, a window appears as shown in Figure 9-29, "Active Users."

Figure 9-30 User Access Log Viewer with Simple Filter



#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1.	2005/11/18	23:34:49	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
2.	2005/11/18	23:30:56	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
3.	2005/11/18	22:53:43	admin	efgh-ultra.cisco.com	Delete	Role	INFO	SecurityActivity	Role newrole1 (id=265810285) is deleted.
4.	2005/11/18	22:49:15	admin	efgh-ultra.cisco.com	Create	Role	INFO	SecurityActivity	Role newrole1 (id=265810285) is created.
5.	2005/11/18	22:10:38	admin	efgh-ultra.cisco.com	Create	Group	INFO	SecurityActivity	Group newgroup1 (id=1203533294) is created.
6.	2005/11/18	21:46:26	admin	efgh-ultra.cisco.com	Modify	Role	INFO	SecurityActivity	Role SysAdminRole (id=-1234592039) is modified.
7.	2005/11/18	21:46:25	admin	efgh-ultra.cisco.com	Create	User	INFO	SecurityActivity	User new1 (id=1794273524) is created.
8.	2005/11/18	21:45:22	admin	efgh-ultra.cisco.com	Delete	User	INFO	SecurityActivity	User new1 (id=1794273524) is deleted.
9.	2005/11/18	21:44:59	admin	efgh-ultra.cisco.com	Modify	Role	INFO	SecurityActivity	Role SysAdminRole (id=-1234592039) is modified.
10.	2005/11/18	21:44:58	admin	efgh-ultra.cisco.com	Create	User	INFO	SecurityActivity	User new1 (id=1794273524) is created.

All the log information about user actions appears.

Note The types of activities or objects to be logged can be configured. This can be done directly through SQL. By default, security-related activities and activities on objects listed in the Role editor are logged.

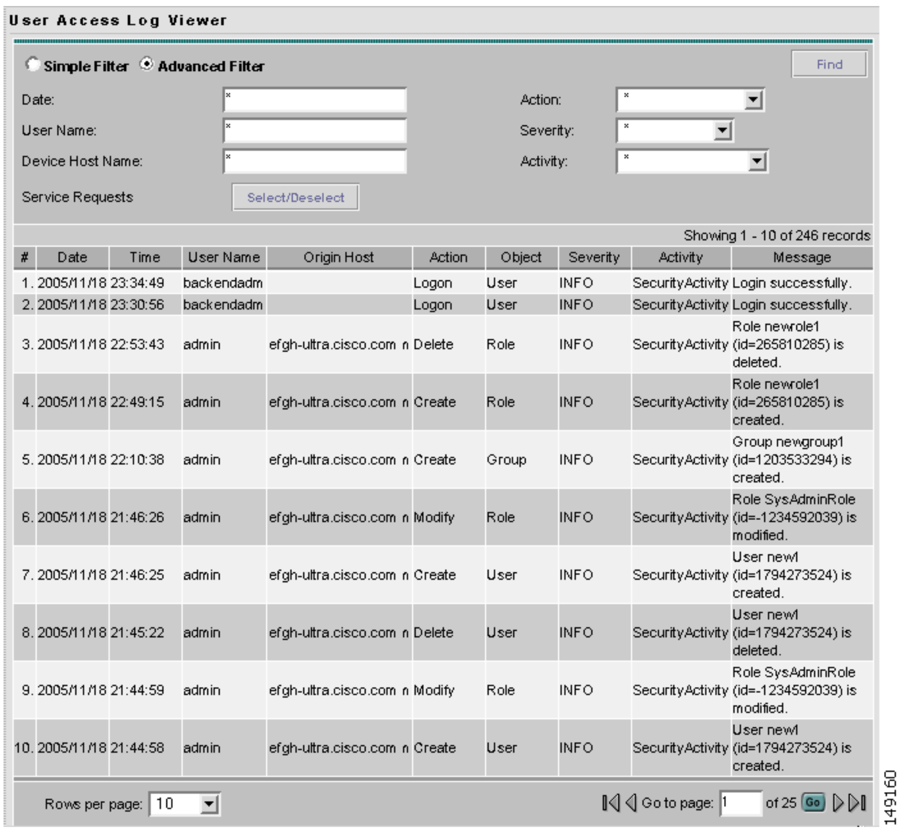
Step 2 The default **Simple Filter** radio button is selected. To filter using the **Simple Filter**, continue with Step 3. To filter using **Advanced Filter**, proceed to Step 5.

Step 3 To filter the information with **Simple Filter**, keep the **Simple Filter** radio button selected and from **Filter By**, choose: **Date**, **User Name**, **Origin Host**, **Action**, **Severity**, or **Activity** (also column names). For **Matches**, enter the beginning characters of what you want to match followed by *****. Then click **Find**. The result is that only the log information matching the entered filter appears.

Step 4 To exit this log report, choose another feature from the main product tabs.

Step 5 To filter the information with **Advanced Filter**, click the **Advanced Filter** radio button. A window as shown in Figure 9-31, "User Access Log Viewer with Advanced Filter," appears.

Figure 9-31 User Access Log Viewer with Advanced Filter



All the log information about user actions appears.

Step 6 Enter filter information you want to match in one or more of the following categories and then click **Find**.

Note When you choose multiple filters, the log results that appear are only the ones that match all the specified filter information.

- **Date** Enter the beginning characters of the date you want to view followed by a ***,** in the format given in the **Date** column.
- **User Name** Enter the beginning characters of the specific **User Name** you want to view followed by a *****.

- **Device Host Name** Enter the beginning characters of the specific **Host Name** you want to view followed by a *.
- **Action** Click the drop-down list and choose from: **UNKNOWN**; **View**; **Create**; **Modify**; **Delete**; **Logon**; **Logoff**; **Session Timeout**. If you decide not to use this filter, just keep *.
- **Severity** Click the drop-down list and choose from: **UNKNOWN**; **INFO**; **WARNING**; **ERROR**. If you decide not to use this filter, just keep *.
- **Activity** Click the drop-down list and choose from: **UNKNOWN**; **SecurityActivity**; or **UserActivity**. The result is that only the log information matching the entered filter appears.

Step 7 **Service Requests** has a selection of **Select/Deselect**. Click this and you receive a list of Service Requests in the system from which you can check check box(es) for the User Access Log to handle. Then click the **Select** button. These Service Requests then appear on Figure 9-31.

Step 8 To exit this log report, choose another feature from the main product tabs.

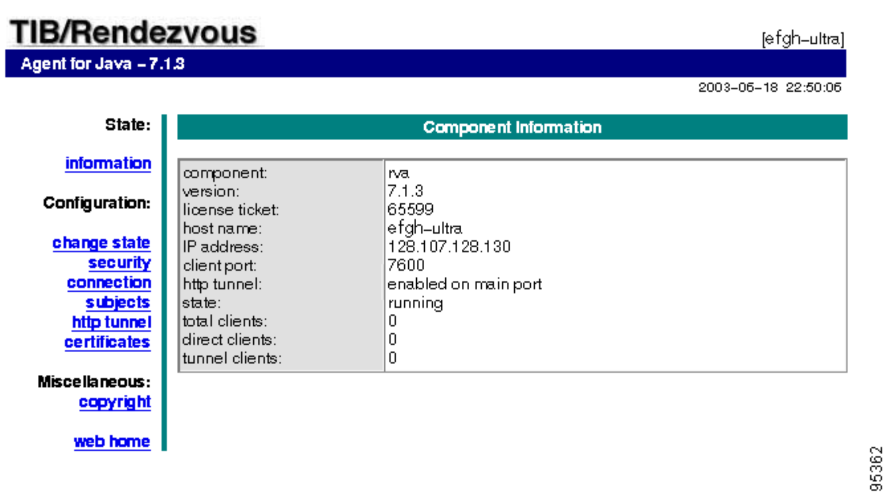
Manage TIBCO Rendezvous

The only reason you would ever use this functionality is if you change the TIBCO ports for TIBCO Rendezvous Agent (rva) or TIBCO Rendezvous Routing Daemon (rvrd) after installation. The changes being made here only affect the topology tool, a Java WebStart application.

Choose **Administration** > **Manage TIBCO Rendezvous** and follow these steps:

Step 1 After you choose **Administration** > **Manage TIBCO Rendezvous**, a window appears as shown in Figure 9-32, "TIBCO Rendezvous."

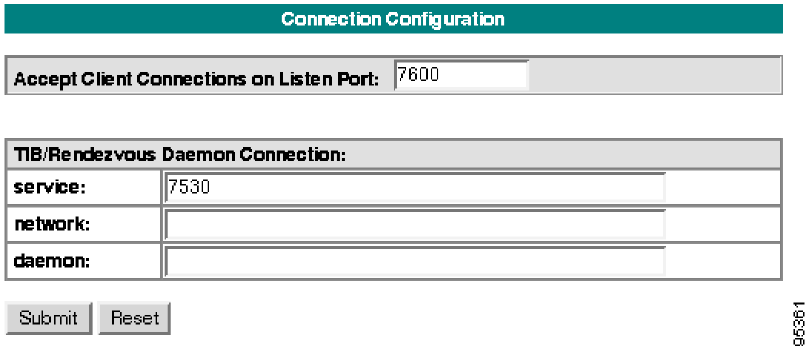
Figure 9-32 TIBCO Rendezvous



Step 2 From Figure 9-32, click **connection**, as described in Step 3; and click **change state**, as described in Step 4. These are choices in the left column of Figure 9-32.

Step 3 In Figure 9-32, when you click **connection**, a window such as Figure 9-33, "Connection Configuration," appears.

Figure 9-33 Connection Configuration



If you must change the **rva** port number from the existing value, change the **Accept Client Connections on Listen Port:** field to your new rva port number for ISC. If you must change the **rvrd** port number from the existing value, change the **service** field to your new rvrd port number for ISC. Then click **Submit**. Then Figure 9-33 returns with the new value and a note that says "Configuration change will take effect after RVA is re-activated. To re-activate RVA set it into idle state and then back to active state."

Step 4 In Figure 9-32, click **change state**, follow the instructions, and you complete this functionality.

Step 5 From a terminal window, change to the **bin** directory of your ISC installation, such as **/opt/isc-5.0/bin**.

Step 6 Source the ISC environment:

- C Shell - use the command **source ./vpnenv.csh**
- K Shell or Bash - use the command **. ./vpnenv.sh**

Step 7 To start the script, at the command line type **updateWebStartJars**.

Step 8 The next time you start a Java WebStart, such as the topology tool, these changes are in effect.