

Administration

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Administration** tab and you receive a window as shown in Figure 8-1, "Administration Selections."

Figure 8-1 Administration Selections

CISCO SYSTEMS	Home Shortcuts Account Index Help IP Solution Center Service Inventory Service Design Monitoring Administration ontrol Center + Active Users + User Access Log +	About Logout User: admin
You Are Here: • Administration		Customer: None
	Administration	
	Tools to manage users and ISC configuration, servers, remote installation, and licensing.	
	Security Create and manage Users, User Groups, User Roles, and Object Groups.	
	Control Center Manage ISC configuration, servers, remote installation, and licensing.	
	Active Users Wewusers currently connected to ISC. Disconnect users.	
	User Access Log Viewthe user access log.	
	Manage TIB CO Rendezvous Specify attributes for proper messaging among all Java ^{ma} Web Start distributed applications.	116244

Then you can navigate to the following selections:

- Security, page 8-2 Create and manage Users, User Groups, User Roles, and Object Groups
- Control Center, page 8-25 Manage ISC configuration, servers, remote installation, and licensing
- Active Users, page 8-37 View users currently connected to ISC. Disconnect users.
- User Access Log, page 8-37 View the user access log.
- Manage TIBCO Rendezvous, page 8-39 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, and user roles 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.

Navigate **Administration** > **Security** to access the user management tools. The window shown in Figure 8-2, "Security Window," appears.

Figure 8-2 Security Window

Cisco Systems	IP So	Home Shortcuts Account Index Help About Log	out
antillinaantillina.		e Inventory Service Design Monitoring Administration User: adi	nin
You Are Here: Administration		Customer: N	one
	Security	<i>(</i>	
Selection - Users - User Groups - User Roles - Object Groups	Create and	manage Users, User Groups, User Roles, and Object Groups. Users Create and manage Users to also access Inventory Manager, Topology, and Northbound API. User Groups Create and manage User Groups. A Group is used to combine the privileges of all the roles contained within it. User Roles Create and manage User Roles, which define a set of permissions.	
		Object Groups Create and manage a group of objects, such as devices, interfaces, and named physical circuits.	116078

From the Security window, navigate to the following:

- Users, page 8-2 to manage users
- User Groups, page 8-8 to manage user groups
- User Roles, page 8-11 to manage user roles
- Object Groups, page 8-18 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 8-22.

Users

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

Step 1 The window in Figure 8-3, "Users Window," appears.

📳 🛄 Users							
CISCO SYSTEMS	IP	s	olution Cen	ter	Home Shortcuts Acc	ount Index Help	About Logout
illinillin	Se	rvi	ice Inventory	Service Desi	gn Monitoring Ac	Iministration	User: admin
 Security 	Control	Ce	nter 🔹 Active User	s 🍳 Uiser Acci	ess Log 🔸		
ou Are Here: • Administration • 3	Security	U	sers				Customer: None
	Use	rs					
Selection Users				Showusers	with User ID 🗾 Ma	tobing ×	Find
- User Groups				3109943613			21 of 21 records
•• User Roles •• Object Groups	#		U ser ID	First Name	Last Name	Work Phone	Mobile Phone
	1.		admin	admin	admin		
	2.		user-collection	Joe	Collection	(123) 456-7890	(123) 456-7890
	3.	Г	user-firewall	Joe	Firewall	(123) 456-7890	(123) 456-7890
	4.		user-firewallserviceop	Joe	FirewallServiceOp	(123) 456-7890	(123) 456-7890
	5.	Г	user-import	Joe	Import	(123) 456-7890	(123) 456-7890
	6.		user-ipsec	Joe	IPSec	(123) 456-7890	(123) 456-7890
	7.	Г	user-ipsecserviceop	Joe	IPSecServiceOp	(123) 456-7890	(123) 456-7890
	8.		user-I2vpn	Joe	L2VPN	(123) 456-7890	(123) 456-7890
	9.	Г	user-l2vpnserviceop	Joe	L2VPNServiceOp	(123) 456-7890	(123) 456-7890
	10.		user-mpls	Joe	MPLS	(123) 456-7890	(123) 456-7890
	11.	Γ	user-mplsserviceop	Joe	MPLSServiceOp	(123) 456-7890	(123) 456-7890
	12.		user-nat	Joe	NAT	(123) 456-7890	(123) 456-7890
	13.	\square	user-natserviceop	Joe	NATServerOp	(123) 456-7890	(123) 456-7890
	14.		user-qos	Joe	QoS	(123) 456-7890	(123) 456-7890
	15.	Γ	user-qosserviceoprole	Joe	QoSServiceOp	(123) 456-7890	(123) 456-7890
	16.		user-sysadmin	Joe	SysAdmin	(123) 456-7890	(123) 456-7890
	17.	Γ	user-te	Joe	TE	(123) 456-7890	(123) 456-7890
	18.		user-teserviceop	Joe	TEServiceOp	(123) 456-7890	(123) 456-7890
	19.	Γ	user-useradmin	Joe	UserAdmin	(123) 456-7890	(123) 456-7890
	20.		user-vpls	Joe	VPLS	(123) 456-7890	(123) 456-7890
	21.	Γ	user-vplsserviceop	Joe	VPLSServiceOp	(123) 456-7890	(123) 456-7890
		Ro	wws per page: All 💌		Id	Gotopage: 1	of 1 💿 👂 🕅
					Details Create	Copy Edit	Delete

Figure 8-3 Users Window

- Step 2 In Figure 8-3, you can filter the list of users (corresponding to the column headings) in which to search, using the drop-down menu for Show users with:
 - User ID user ID used for logging into ISC
 - First Name user's first name
 - Last Name user's last name
 - Work Phone user's work phone number
 - Mobile Phone user's cell phone or mobile phone number.

Enter the search criteria, using * if you want, and click Find.



The search tool is case-sensitive.

Step 3	At the bottom of the window, you can change the number of rows shown on this window in Rows per
	page.
Step 4	The explanations of the remainder of the buttons are given as follows:

- Details, page 8-4 View a User Detail Report
- Create, page 8-4 Create a new user
- Copy, page 8-7 Make a copy of an existing user and make changes to create a new user
- Edit, page 8-7 Edit selected user
- Delete, page 8-7 Delete selected user(s).

Details

The **Details** button, located at the bottom of Figure 8-3, has 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. Navigate Administration > Security > Users and click the Details button.

Create

The **Create** button, located at the bottom of Figure 8-3, allows a user with the required privileges to create a new user. Follow these steps:

Step 1 Navigate Administration > Security > Users.

Step 2 Click the Create button and the window shown in Figure 8-4, "Create/Edit Users Window," appears.

Security			
User ID [*] :			
Password [*] :			
Verify Password [*] :			
Permissions for Others:	View	🔽 Edit	🗌 Delete
User Groups:			Edit
Assigned Roles:			Edit
Personal Information			
Full Name [*] :			
Work Phone:			
Mobile Phone:			
Pager:			
Email:			
Location:			
Supervisor Information:			
User Preferences			
Language:	English	•	
Rows per page:	10 💌		
Logging Level:	Warning 💌		
Initial Screen:	Home	•	
			Save Cancel
			Save Cancel

Figure 8-4 Create/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
- Verify Password (required) Confirm by re-entering the selected password
- **Permission for Others** Select 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 will be 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 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, select the check box next to each group to which you want to add this user or select the check box in the header row to add the user to all the groups shown. 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 10).

• Assigned Roles Click Edit and you receive a list of the roles. You can filter this list. From the selected roles, select the check box next to each role to which you want to assign this user or select the check box in the header row to assign all the shown roles to the 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 menu 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.
 - E-mail (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 menu 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, and All.
 - 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**. This is a way to specify the first screen you will see after logging in.
- Step 6 Click Save. Figure 8-3 reappears with the new user listed.

Сору

The **Copy** button, located at the bottom of Figure 8-3, 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 Navigate Administration > Security > Users.
- Step 2 Select 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 8-4, "Create/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 8-4.
- Step 6 Click Save and you will return to Figure 8-3. 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 8-3, allows a user with the required privileges to edit user-specific information. Follow these steps:

- Step 1 Navigate Administration > Security > Users.
 Step 2 Select 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 8-4, "Create/Edit Users Window," appears.

٩,

- **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 Step 3 of the "Create" section on page 8-4.
- Step 5 Click Save. Figure 8-3 reappears with the edited user listed.

Delete

The **Delete** button, located at the bottom of Figure 8-3, allows a user with the required privileges to delete user-specific information. Follow these steps:

Step 1Navigate Administration > Security > Users.Step 2Select the check box(es) for the row(s) of the user(s) you want to delete or select the check box in the
header row to select all the users for deletion.Step 3Click the Delete button and a window as shown in Figure 8-5, "Users Confirm Delete" appears.

Figure 8-5 Users Confirm Delete

Confirm Delete							
Showing 1-1 of 1 records							
# User ID	Name						
1. new1	newfirstname1 newname1						
Rows per page: 10 💌							
	Delete Cancel						

- Step 4 Click Delete to continue with the process of deleting information for the specified user(s). Otherwise click Cancel.
- Step 5 Figure 8-3, "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, navigate **Administration** > **Security** > **User Groups** and follow these steps:

Step 1 The window in Figure 8-6, "User Groups Window" appears.

Figure 8-6 User Groups Window

🔮 📠 User Groups					
CISCO SYSTEMS			Home Shortcuts	Account Index Help	About Logout
	IP Solution Cer	nter			
	Service Inventory	Service Design	Monitoring	Administration	User: admin
♦ Security ♦ Co	ntrol Center 🔹 Active Use	rs 🔸 User Access L	og 🔸		
You Are Here: Administration Se	curity • User Groups				Customer: None
	User Groups				
Selection		Show groups wit	h Name 💌	Matching	Find
• User Groups • User Roles					ving 0 of 0 records
• Object Groups	# N	lame		Description	
	Rows per page: All 🔻	[🛛 🗐 🕼 Go to page: 🛛 1	of 1 💿 🖓 🕅

- Step 2 In Figure 8-6, you can filter the list of user groups (corresponding to the column headings) in which to search, using the drop-down menu for Show groups with:
 - Name
 - Description

Enter the search criteria, using * if you want, and click Find.

The search tool is case-sensitive.

- Step 3 At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**.
- Step 4 The explanations of the remainder of the buttons is given as follows:
 - Create, page 8-9 Create a new user group
 - Edit, page 8-10 Edit selected user group
 - Delete, page 8-10 Delete selected user group(s)

Create

The **Create** button, located at the bottom of Figure 8-6, allows a user with the required privileges to create a user group. Follow these steps:

- Step 1 Navigate Administration > Security > User Groups.
- Step 2 Click the Create button and the window shown in Figure 8-7, "Create/Edit User Groups Window," appears.

Figure 8-7 Create/Edit User Groups Window

Name [*] :		
Description:		
Roles:	Edit	
Users:	Edit	
	Save Cancel	937 47

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, select the check box next to each role you want to attach to this user group or select the check box in the header row to assign all the shown roles 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, select the check box next to each user you want to attach to this user group or select the check box in the header row to assign all the shown users to this user group. Then click OK. You can repeat this procedure if you want to change your selection.

Step 4 Click Save. Figure 8-6 reappears with the new user group listed.

Edit

The **Edit** button, located at the bottom of Figure 8-6, allows a user with the required privileges to edit user group-specific information. Follow these steps:

Step 1 Navigate Administration > Security > User Groups.
Step 2 Select 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 8-7, "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 8-9.
Step 5 Click Save. Figure 8-6 reappears with the edited user group list.

Delete

The **Delete** button, located at the bottom of Figure 8-6, allows a user with the required privileges to delete user group-specific information. Follow these steps:

Step 1 Navigate Administration > Security > User Groups.

- Step 2 Select the check box(es) for the row(s) of the user group(s) you want to delete or select the check box in the header row to select all the user groups for deletion.
- Step 3 Click the Delete button and a window as shown in Figure 8-8, "User Groups Confirm Delete," appears.

Figure 8-8 User Groups Confirm Delete

Confirm Delete							
	Showing 1-1 of 1 records						
#	Name	Description					
1. г	newgroup1	description for newgroup1					
Rows	s per page: 10 💌	Ī					
		Delete Cancel					

- Step 4 Click Delete to continue the process of deleting information for the specified user group(s). Otherwise click Cancel.
- Step 5 Figure 8-6, "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 on 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.



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, navigate **Administration** > **Security** > **User Roles** and follow these steps:

Step 1 The window in Figure 8-9, "User Roles Window," appears.

User Roles				
Cisco Systems				Home Shortcuts Account Index Help About Logout
	IP	S	olution Cente	
			U	rvice Design Monitoring Administration User: admin
◆ Security ◆ C	ontrol	Cer	nter 🔸 Active Users 🤸	• User Access Log •
u Are Here: Administration S				Customer: Non
1611 104F11	Use	≥r R	oles	
Selection •Users				Viewroles with Name I Matching * Find
User Groups				Showing 1 - 20 of 20 records
User Roles Object Groups	#		Name	Description
	1.	Г	CollectionRole	ISC predefined role. It has the permission to run collection on devices.
	2.		DeviceImportRole	ISC predefined role. It has the permission to import devices.
	З.	Γ	FirewallRole	ISC predefined role. It has the permission to manage Inventory and deploy Firewall Service Request.
	4.	Γ	FirewallServiceOpRole	ISC predefined role. It has the permission to deploy Firewall Service Request.
	5.	Γ	IPsecRole	ISC predefined role. It has the permission to manage Inventory and deploy IPsec Service Request.
	6.	Γ	IPsecServiceOpRole	ISC predefined role. It has the permission to deploy IPsec Service Request.
	7.	Γ	L2VPNRole	ISC predefined role. It has the permission to manage Inventory and deploy L2VPN Service Request.
	8.		L2VPNServiceOpRole	ISC predefined role. It has the permission to deploy L2VPN Service Request.
	9.	Γ	MPLSRole	ISC predefined role. It has the permission to manage Inventory and deploy MPLS Service Request.
	10.	Γ	MPLSServiceOpRole	ISC predefined role. It has the permission to deploy MPLS Service Request.
	11.		NATRole	ISC predefined role. It has the permission to manage Inventory and deploy NAT Service Request.
	12.	Γ	NATServiceOpRole	ISC predefined role. It has the permission to deploy NAT Service Request.
	13.		QoSRole	ISC predefined role. It has the permission to manage Inventory and deploy QoS Service Request.
	14.	Γ	QoSServiceOpRole	ISC predefined role. It has the permission to deploy QoS Service Request.
	15.	Γ	SysAdminRole	ISC predefined role. It has full permission.
	16.		TERole	ISC predefined role. It has the permission to manage Inventory and deploy TE Service Request.
	17.		TEServiceOpRole	ISC predefined role. It has the permission to deploy TE Admission Service Request.
	18.	Γ	UserAdminRole	ISC predefined role. It has full permission to manage User, Group and Role.
	19.	Γ	VPLSRole	ISC predefined role. It has the permission to manage Inventory and deploy VPLS Service Request.
	20.		VPLSServiceOpRole	ISC predefined role. It has the permission to deploy VPLS Service Request.
		Ro	ws per page: 🛛 All 💌	🖉 🕄 Go to page: 📔 🛛 of 1 🚥 🕞 []
				Create Copy Edit Delete

Figure 8-9 User Roles Window

The predefined roles shown in Figure 8-9 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 In Figure 8-9, you can filter the list of user roles (corresponding to the column headings) in which to search, using the drop-down menu for Show roles with:
 - Name
 - Description

Enter the search criteria, using * if you want, and click Find.

Tł	ne search tool is case-sensitive.				
	t the bottom of the window, you can change the number of rows shown on this window in Rows per nge .				
The explanations of the remainder of the buttons is given as follows:					
•	Create, page 8-14 Create a new user role				
•	Copy, page 8-17				
•	Edit, page 8-17 Edit selected user role				

• Delete, page 8-18 Delete selected user role(s)

Create

The **Create** button, located at the bottom of Figure 8-9, allows a user with the required privileges to create a new user role. Follow these steps:

- Step 1 Navigate Administration > Security > User Roles.
- Step 2 Click the Create button and a window comprised of Figure 8-10, "Create/Edit User Roles Window (Top)," and Figure 8-11, "Create/Edit User Roles Window (Bottom)," appears.

Figure 8-10 (Create/Edit U	ser Roles	Window ((Top)
---------------	---------------	-----------	----------	-------

Name [*] :	
Enable Object Group Association:	
Parent Role:	Edit
Customer:	Edit
Provider:	Edit
Object Groups:	Edit
Description:	_
Users:	Edit
User Groups:	Edit

Resource	All	Create	View	Edit	Delete
Persistent Task					
SAA Probe					
Workflow					
Device					
ISC Host					
Customer					
Provider					
PE					
CPE					
QoS Policy					
QoS Service Request					
MPLS Policy					
MPLS Service Request					
L2VPN Policy					
L2VPN Service Request					
Firewall Policy					
Firewall Service Request					
NAT Service Request					
IPsec Policy					
IPsec Service Request					
Deployment Flow					
Template					
TE Provider					
TE Router					
TE Tunnel Policy					
TE Tunnel & Resource Service Request					
TE Traffic Admission Service Request					
VPLS Policy					
VPLS Service Request					
Service Order					
Object Group					

Figure 8-11 Create/Edit User Roles Window (Bottom)

Step 3 Enter the following information in Figure 8-10:

- Name (required) Enter the name of this new user role.
- Enable Object Group The default is that this check box is deselected. In this case, Parent Role, Customer, and Provider are enabled and Object Groups is not enabled. Figure 8-11 is complete as shown. If you select this check box, Parent Role, Customer, and Provider are not enabled and Object Groups is enabled. Figure 8-11.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 8-9, 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.



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, click the radio button for the object group(s) you want to select 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 8-9.
- Users (optional) Click Edit and a list of the existing users appears. You can filter this list. From the selected users, select the check box(es) for the user(s) you want assigned to this role or select the check box in the header row to assign all the users to this role. Then click OK. You can repeat this procedure if you want to change your selection.



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, select the check box(es) for the user group(s) you want assigned to this role or select the check box in the header row to assign all the user groups to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.
- Step 4

In Figure 8-11, click any combination of the following permissions: Create; View; Modify; Delete. If you want all the permissions, click All.



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.



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**.



The Workflow object is currently not used.

Step 5 Click Save. Figure 8-9 reappears with the new user role listed.

Сору

The **Copy** button, located at the bottom of Figure 8-9, 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 Navigate Administration > Security > User Roles.
- Step 2 Select 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 8-10, "Create/Edit User Roles Window (Top)," and Figure 8-11, "Create/Edit User Roles Window (Bottom)" appears.
- Step 4 Required entries are 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 8-14.
- Step 6 Click Save and you will return to Figure 8-9. 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 8-9, allows a user with the required privileges to edit user role-specific information. Follow these steps:

- Step 1 Navigate Administration > Security > User Roles.
- Step 2 Select 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 8-10 and Figure 8-11 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 8-14.
- Step 5 Click Save. Figure 8-9 reappears with the edited user roles listed.

Delete

The **Delete** button, located at the bottom of Figure 8-9, allows a user with the required privileges to delete user role-specific information. Follow these steps:

- Step 1 Navigate Administration > Security > User Roles.
- Step 2 Select the check box(es) for the row(s) of the user role(s) you want to delete or select the check box in the header row to select all the users for deletion.
- Step 3 Click the Delete button and a window as shown in Figure 8-12, "User Roles Confirm Delete," appears.

Figure 8-12 User Roles Confirm Delete

	Confirm Delete
	Showing 1-1 of 1 records
# Name	Description
1. newrole1	
Rows per page: 20 💌	
	Delete Cancel 25

- Step 4 Click Delete to continue with the process of deleting information for the specified user role(s). Otherwise click Cancel.
- Step 5 Figure 8-9, "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 multiple Object Groups. A role can be associated with either Object Group(s), or a Customer, a Provider, but not both. 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 that 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 8-22.

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 you intention is to limit access to a scope of devices or NPCs, define a role to be associated with Object Group(s), Device, CE, PE, and NPC.

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

Step 1 The window in Figure 8-13, "Object Groups Window," appears.

Figure 8-13 Object Groups Window

🕘 🛛 🔤 Object Groups					
CISCO SYSTEMS		F	iome Shortcuts A	Account Index Help	About Logout
	IP Solution Ce	nter			
	Service Inventory	Service Design	Monitoring	Administration	User: admin
♦ Security ♦ Co	ontrol Center 🔸 Active Use	ers 🔸 User Access Li	og 🔸		
You Are Here: Administration Se	ecurity > Object Groups				Customer: None
	Object Groups				
Selection • Users		Show groups with	n Name 💌	Matching ×	Find
User Groups User Roles					g1-1 of1 record
• Object Groups	#	Name		Description	
	1. TiosCEAnd	/PNSM3Group			
	Rows per page: 10 💌	1		🛛 🗐 Gotopage: 🛛	of 1 💿 🖓 🕅
				Create Edit	Delete

- Step 2 In Figure 8-13, you can filter the list of object groups (corresponding to the column headings) in which to search, using the drop-down menu for Show groups with:
 - Name
 - Description

Enter the search criteria in Matching, using * if you want, and click Find.

The search tool is case-sensitive.
At the bottom of the window, you can change the number of rows shown on this window in Rows per page .
The explanations of the remainder of the buttons is given as follows:
• Create, page 8-14 Create a new object group
• Edit, page 8-17 Edit a selected object group
• Delete, page 8-18 Delete selected object group(s)

Create

The **Create** button, located at the bottom of Figure 8-13, allows a user with the required privileges to create a new object group. Follow these steps:

- Step 1 Navigate Administration > Security > Object Groups.
- Step 2 Click the Create button and the window Figure 8-14, "Create/Edit Object Group Window," appears.

Name [*] :			
Description:			
PE Group Members:	# Name	Interface Members	Edit
	1.ios-pe102		
	2. ios-pe101		
	Rows per page: 10 💌	🛛 🕄 Go to page: 📔 of 1 💿 🕞 🕅	
CE Group Members:	# Name	Interface Members	Edit
	1.sec4-cat6k_VPNSM_3	FastEthernet2/1,FastEthernet2/10	
	Rows per page: 10 💌	【↓ Go to page: 1 of 1 Go	
NPC Group Members:	#	Name	Edit
	Rows per page: 10 💌	∥	
		Save	Cancel

Figure 8-14 Create/Edit Object Group Window

Step 3 Enter the following information in Figure 8-14:

- 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, click the radio button 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 8-14, "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, click the radio button 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 will be empty. All existing interfaces for each of the CE 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 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 8-14, "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 Named Physical Circuits (NPCs) appears. You can filter this list. From the selected NPCs, click the radio button 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 will return to Figure 8-14, "Create/Edit Object Group Window," and the Name for each NPC Group Member appears.
- Step 4 Click Save. Figure 8-14 reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of Figure 8-14, allows a user with the required privileges to edit object group-specific information. Follow these steps:

Step 1	Navigate Administration > Security > Object Groups.
Step 2	Select 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 8-14, 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 8-20.
Step 5	Click Save. Figure 8-14 reappears with the edited object groups listed.

Delete

The **Delete** button, located at the bottom of Figure 8-14, allows a user with the required privileges to delete object group-specific information. Follow these steps:

- Step 1 Navigate Administration > Security > Object Groups.
- Step 2 Select the check box(es) for the row(s) of the object group(s) you want to delete or select the check box in the header row to select all the object groups for deletion.
- Step 3 Click the Delete button and a window as shown in Figure 8-15, "Delete Object Groups Confirm Delete," appears.

Figure 8-15 Delete Object Groups Confirm Delete

Delete Object	Group(s)
	C	onfirm Delete
		Showing 1 - 2 of 2 records
#	Name	Description
1.	objgp2	
2.	objgp3	
Rows per pag	e: All 💌	【↓ Go to page:
		Delete Cancel

- Step 4 Click Delete to continue with the process of deleting information for the specified object group(s). Otherwise click Cancel.
- Step 5 Figure 8-14, "Create/Edit Object Group 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 8-22
- Illustration of Setup, page 8-23
- Steps to Set Up Example, page 8-24

Example

This section explains an example data center for which the following sections, "Illustration of Setup" section on page 8-23 and "Steps to Set Up Example" section on page 8-24 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 8-16, "Contents in Example," shows the setup described in the "Example" section on page 8-22.



Figure 8-16 Contents in Example

Steps to Set Up Example

This section explains the steps to create the example explained in the "Example" section on page 8-22 and shown in the "Illustration of Setup" section on page 8-23.

- Step 1 Create the following Object Groups (see the "Create" section on page 8-20, 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 8-14, 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 8-11.
 - 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 8-2.
 - 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 remotely install and uninstall a Processing server, Collection server, or Interface server; how to define collection zones; and how to install license keys.

Navigate **Administration > Control Center** and you go to the default page of **Hosts** in the TOC, as shown in Figure 8-17, "Control Center > Hosts."

Figure 8-17 Control Center > Hosts

CISCO SYSTEMS	IF	Solution Ce	nter		I	Home Shortcuts /	Account Index Help	About Logout
atilitaatilitaa • Security • Con		ervice Inventory I Center → Active Us			ring Admin	istration		User: admin
You Are Here: Administration Co								Customer: None
Selection • Hosts • Collection Zones	Ho	sts					Showin	Refresh
• Licensing	#	V N	ame	Role	S	tart Time	Stop Time	Running
	1.	smilley-ultra.cisco.c	om	Master	Jan 29 03:40:55 PN	I PST	UNKNOWN	Yes
		Rows per page: All	·			l	🛛 🎝 Go to page: 🛛	of 1 💿 🖓 🕅
			Detail	s Con	ig Servers	Watchdog	nstall Uninstall	Logs 🔻

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

- Hosts, page 8-25 Hosts allows you to manage the various servers.
- Collection Zones, page 8-32 Collection Zones are the means of associating collection servers with network devices.
- Licensing, page 8-34 Licensing is where you install license keys, which is the only way to access services and APIs.

Hosts

Navigate Administration > Control Center > Hosts.

A window as shown in Figure 8-17 appears.



Only the **Install** and **Logs** buttons are enabled by default when there is no host selected. When one or more hosts are selected by selecting the check boxes, the Install and Logs buttons are disabled and the other buttons are enabled.

Click any of the buttons and proceed as follows:

- Details, page 8-26 Available only when one host system is chosen.
- Config, page 8-27 Available only when one or more host systems are chosen.
- Servers, page 8-28 Available only when one or more host systems are chosen.
- Watchdog, page 8-29 Available only when one or more host systems are chosen.
- Install, page 8-30 Available only when no host system selections are made.
- Uninstall, page 8-31 Available only when one host system is chosen.
- Logs, page 8-31 Available only when no host system selections are made.

Details

For details about a chosen host, do the following:

Step 1 Choose a host by selecting 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 8-18, "Host Details." This shows the details about the chosen host.

Figure 8-18 Host Details

Host Details

	a10.cisco.com
General	
Active:	Yes
Image:	isc3.0-20030406.00.Q
Registered Date:	May 21 03:29:10 PDT
UnRegistered Date:	
Install Location:	/disk2/opt/iscadm/isc3
Install Time:	2003-03-19 16:59:07.
Locations	
Server Logs:	/disk2/opt/iscadm/isc3
Task Logs:	/disk2/opt/iscadm/isc3
Temporary:	/disk2/opt/iscadm/isc3
Disk Stats	
Path:	/disk2/opt/iscadm/isc3
Total Disk Space:	19146 MB
Free Disk Space:	12810 MB; 66% Free
Path:	/disk2/opt/iscadm/isc3
Total Disk Space:	19146 MB
Free Disk Space:	12810 MB; 66% Free
Health Stats	
Last Heartbeat:	
Last Heartbeat Status:	
Last Heartbeat Duration:	
Collection Zones	
(<u> </u>	•

Step 3 Click **OK** and you return to Figure 8-17.

Config

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



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

- Step 1 From Figure 8-17 on page 8-25, select 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 8-19, "Properties," appears. It is a list of all the folders with all the properties. See Appendix B, "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 8-19 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 8-20, "Properties Detail Example."

Host Configuration Version: Apr 22 04:56:09 PDT Autodiscovery Cleanup RuntimeTasks TaskLogs	Attribute Cle	anup\logLevel	Version Apr 22 04:56:09 PDT
TempFiles JogLevel DCS DeploymentFlow OS GSAM GTL GUI Cul GUI DistributionFramework GUI GUI GUI GUI GUI GUI SLA GSLA SYSTEM	Description:	for a component. logLevel is the level a	ue)
E Scheduler	Current Value	e:	
	New Value:	SEVERE 💌	
E _ VpnInvServer			
🗄 🚞 aagent			Set Property Reset Property
⊞ 🗋 dtd	·		
Create Version Set To Latest			

Figure 8-20 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 menu 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, do the following:

- Step 1 From Figure 8-17 on page 8-25, select 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 8-21, "Servers," appears.

								Refresh
							S	howing 1 - 9 of 9 records
# [Name	State	Generation	Start Time	PID	Successful Heartbeats	Missed Heartbeats
1. [-	cornerstonebridge	started	1	Jan 29 03:41:03 PM PST	527	22703	0
2. [worker	started	1	Jan 29 03:41:03 PM PST	530	22566	0
з. Г	-	dispatcher	started	1	Jan 29 03:41:03 PM PST	528	22661	0
4. [lockmanager	started	1	Jan 29 03:41:03 PM PST	529	22549	0
5. J	-	nspoller	started	1	Jan 29 03:40:57 PM PST	0	22709	0
6. [scheduler	started	1	Jan 29 03:43:46 PM PST	550	22565	0
7. [-	httpd	started	2	Jan 29 03:45:19 PM PST	556	22716	0
8. [dbpoller	started	1	Jan 29 03:40:57 PM PST	0	22637	0
		cnsserver	started	1	Jan 29 03:41:03 PM PST	526	22522	0

Figure	8-21	Servers

- Step 3 Select 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 8-21.
- 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 8-21, you return to Figure 8-17 on page 8-25.

Watchdog

To view the log information about WatchDog, do the following:

- Step 1 From Figure 8-17 on page 8-25, select 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 8-22, "WatchDog Logs," appears.

Figure 8-22 WatchDog Logs

Name	Size	Last Modified
watchdog.0	255110	Thursday, January 29, 2004 3:45:35 PM PST
watchdog.1	193363	Thursday, January 29, 2004 1:28:30 PM PST

- 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 8-22.
- Step 4 You can repeat the process inStep 3 or click **OK** to return to Figure 8-17 on page 8-25.

Install

You can remotely install the Processing Server, Collection Server, or Interface Server, as follows:



Telnet and ftp *must* be available on both the Master and remote server.

Note	

In this remote install, you *must* accept the default values, similar to the **express** install. If you want to do a **custom** install, it is only available through the installation procedure explained in the "Installing ISC" section of Chapter 2 of *Cisco IP Solution Center Installation Guide, 4.0*

Step 1 From Figure 8-17 on page 8-25, be sure that no check boxes are selected and then click the Install button.

Step 2 A window as shown in Figure 8-23, "Remote Install," appears.

Figure 8-23 Remote Install

Remote Install					
Host Name [*] :					
ISC User [*] :					
ISC User Password [*] :	****				
Role:	Processing Server 💌				
Install Location:					
Root Password:					
	Install Cancel				

- Step 3 Provide the following information in Figure 8-23.
 - Host Name (required)
 - **ISC User** (required) This same user *must* be created on the remote server.



Be sure you have 1 GB of disk space available in the ISC User's home directory.

- ISC User Password (required)
- Role Accept the default of Process Server or click the drop-down menu and choose the Collection Server or Interface Server option.
- Install Location (required)
- Root Password (optional) To auto start ISC on a remote server, the root password is required.

- Step 4 Click the **Install** button.
- Step 5 The result is an Install Log.

Uninstall

You can remotely uninstall the Processing Server, Collection Server, or Interface Server, as follows:

- Step 1 From Figure 8-17 on page 8-25, select a check box next to a host name for which you want to uninstall and then click the **Uninstall** button.
- Step 2 A window as shown in Figure 8-24, "Remote Uninstall," appears.

Figure 8-24 Remote Uninstall

ISC User [*] :			
ISC User Password [*] :	****		
		<u>Uninstall</u>	Cancel 4

- Step 3 Provide the following information in Figure 8-24.
 - ISC User (required)
 - ISC User Password (required)
- Step 4 Click the Uninstall button.
- Step 5 The result is an Uninstall Log.

Logs

You can view install and uninstall logs for the Master and remotely installed server, as follows:

- Step 1 From Figure 8-17 on page 8-25, be sure that no check boxes are selected.
- Step 2 Click the Logs drop-down menu 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 8-17 on page 8-25.

Collection Zones

Navigate Administration > Control Center.

A collection zone is a geographical grouping of devices. Each collection zone is associated with exactly one Collection server that collects data from its devices. However, a Collection server can service multiple collection zones. For example, if you initially create several collection zones and have them all serviced by the Master server, then as the number of devices in each zone grows, you can install additional Collection servers and assign some of the zones to them.

When you install a new Collection server or Processing server, the system creates a new collection zone with the same name as the server. This functionality is for your convenience. You can delete this collection zone if this does not fit your distribution environment setup.

To define collection zones, do the following:

Step 1 From the Control Center, choose Collection Zones from the TOC in the left column, as shown in Figure 8-25, "Choose Control Center > Collection Zones.".

CISCO SYSTEMS	IP S	olution Cei	nter	H	ome Shortcuts	Account Ind	lex Help Abo	ut Logout
illiliinilliliin	Servi	ce Inventory	Service De	sign	Monitoring	Administ	ration	Jser: admin
🗸 🗸 Security 🔸	Control Ce	nter 🔸 Active Use	ers 🗢 User A	ccess Li	og 🔸			
You Are Here: Administration	Control Cent	er • Hosts					Cus	tomer: None
	Hosts							
Selection •• Hosts							[Refresh
 Collection Zones 							Showing 1 - 1	of1 record
Licensing	#	Name		Role	Start Ti	ne	Stop Time	Running
	1. 🥅	smilley-ultra.cisco.co	m Ma	ster Ja	an 29 03:40:55 PM	PST	UNKNOWN	Yes
	Ro	ws per page: All 💌	ĺ			🛛 🖉 🖓 Go to p	bage: 1 of 1	<u>∞</u> ⊳⊳1
		Details	Config	Gervers	Watchdog	Install	Uninstall	ogs 🔻

Figure 8-25 Choose Control Center > Collection Zones

Step 2 A window as shown in Figure 8-26, "Collection Zones," appears.

Figure 8-26 Collection Zones

	Show Collection Zones with Collection Zone Name 💌 matching *								
	Showing 1-1 of 1 records								
#		Collection Zone Name	Collection Host	Description	Devices				
1.		zone1	efgh-ultra.cisco.com	com Created on Fri May 30 17:49:33 PDT 2003 By efgh-ultra.cisco.com					
R	Rows per page: 10 💌								
				<u>Create</u> Edit Delete	Devices				

- Step 3 To Create a collection zone, proceed to Step 4. To Edit a collection zone, proceed to Step 7. To Delete a collection zone, proceed to Step 9. To display the Devices, proceed to Step 12.
- Step 4 From Figure 8-26, without selecting any check boxes, click the Create button.

Step 5 A window as shown in Figure 8-27, "Create Collection Zone," appears.

Figure 8-27 Create Collection Zone

Create Collection Z	one
Name [*] :	
Description:	Created on Mon Jun 09 01:12:38 PDT 2003 By efgh-ultra.cisco.com
Collection Host:	tbigelow-u10.cisco.com 💌
	Save Cancel
Note: - Required	Field

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 menu if you want to select a different collection host.
- Step 6 Click Save. Figure 8-26 reappears, the newly created collection zone is added and a Status appears with a green check in Succeeded. You can repeat Step 4 to Step 6 to create another collection zone. For Edit, proceed to Step 7. For Delete, proceed to Step 9. For Devices, proceed to Step 12.
- Step 7 To edit a collection zone, in Figure 8-26, select the check box for the collection zone you want to edit and then click the Edit button.
- Step 8 A window as shown in Figure 8-27 appears. Follow the instructions in Step 5 and Step 6.
- Step 9 To delete a collection zone, in Figure 8-26, select one or more check boxes for the collection zone(s) you want to delete. You can select all the collections zones by selecting the check box in the header row. Then click the **Delete** button.
- Step 10 A Confirm Delete window appears to give you a chance to click **Cancel** and not delete or to click **OK** and delete.
- Step 11 Figure 8-26 reappears and the collection zone is removed. You can repeat Step 9 and Step 10 to delete more collection zones, you can proceed to Step 3 to create a collection zone, you can proceed to Step 7 to edit a collection zone, or you can proceed to Step 12 to display and assign devices.
- Step 12 To display, add, or delete devices, in Figure 8-26, select a check box for the desired collection zone. Then click the **Devices** button.
- Step 13 A window appears as shown in Figure 8-28, "Collection Zone Devices." This window shows the current devices assigned to the selected collection zone.

Figure 8-28 Collection Zone Devices

Collection Zone Devices

	Show Devices with Any 💌 matching * 🗾 Find							
Showing 1-1 of 1 record								
# 🗆	Device Name	Collection Zone Name	IP Address	Role	Туре			
1. 🖂	newdevice1	null		CE	IE2100			
Rows	Rows per page: 10 💌							
				Add Delete	OK Cancel			

- Step 14 You can filter the list of devices shown by selecting from the Show Devices with drop-down menu, entering what you want to match in matching, and then clicking Find. 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 15 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 16 Figure 8-28 reappears with the updated device information for the selected collection zone.
- Step 17 When Figure 8-28 has all the devices you want, click **OK** and Figure 8-26 reappears with the updated information.

Licensing

Navigate Administration > Control Center.



To enable Traffic Engineering Management (TEM), you need to install a permanent license file. You need to replace the *<install_directory>/thirdparty/parc/installed/data/system.properties* file with the *<distribution_directory>/permLic_system.properties* file. For example: cp permLic_system.properties *<install_directory>/thirdparty/parc/installed/data/system.properties* system.properties

To install license keys, do the following:

Step 1 From Control Center, choose Licensing from the TOC in the left column, as shown in Figure 8-29, "Choose Control Center > Licensing."

CISCO SYSTEMS	IP	s s	olution Ce	nter		Home Shortc	uts Account	Index Help	About Logou
illiimmilliim -	S	ervi	ce Inventory	Servi	ce Design	Monitorii	ng Admini	istration	User: admir
🗸 🗸 Security 🔸 C	ontro	I C e	nter 🔹 Active Us	ers 🕹 L	lser Access	:Log 🗸			
ou Are Here: • Administration >	Control	Cent	er • Hosts						Customer: Non
	Ho	sts							
Selection • Hosts									Refresh
Collection Zones Licensing		_						-	- 1 of 1 record
	#		Name		Role	Sta	nt Time	Stop Tim	e Running
	1.	${{\sqsubset}}$	smilley-ultra.cisco.co	m	Master	Jan 29 03:40:55	PM PST	UNKNOWN	Yes
		Ro	∿s perpage: All 💌	Ī			∎{ Go	to page: 1	of 1 💿 🖓 🕅
			Details	Config	Servers	Watchdog	Install	Uninstall	Logs 🔻

Figure 8-29 Choose Control Center > Licensing

Step 2 From the Installed Licenses table, click the Install button, as shown in Figure 8-30, "Install Button." The Installed Licenses table explains the current statistics. The columns of information tell the Type of license keys that you have installed (API-L2VPN, API-L3MPLS, API-SEC (This feature is NOT SUPPORTED in this release.), IPSEC (This feature is NOT SUPPORTED in this release.), FIREWALL (This feature is NOT SUPPORTED in this release.), L2VPN, L3MPLS/VPN, NAT (This feature is NOT SUPPORTED in this release.), QOS, TE, TE/BRG, TE/RG, VPLS); the Size, which is valid for the ACTIVATION (licensed maximum global count of services) 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).



When you purchase Traffic Engineering Management (TEM), you automatically receive **TE**, **TE/BRG**, and **TE/RG** licenses and an unlimited VPN license. All of these licenses *must* be installed to use the TEM function. The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM; the **TE/RG** license enables primary tunnel placement; and the **TE/BRG** license enables the Fast ReRoute (FRR) protection function.



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

	Installed Licenses						
Туре	Size	Usage	Date Updated				
ACTIVATION	25	4	2004-12-20 16:06				
API-L3MPLS			2004-12-20 16:06				
FIREWALL			2004-12-20 16:06				
IPSEC			2004-12-20 16:06				
L2VPN		4	2004-12-20 16:06				
L3MPLSA/PN			2004-12-20 16:06				
NAT			2004-12-20 16:06				
QOS			2004-12-20 16:06				
TE	25		2004-12-20 16:06				
TE/BRG			2004-12-20 16:06				
TE/RG			2004-12-20 16:06				
VPLS			2004-12-20 16:06				
VPN	50	1	2004-12-20 16:06				
VPN	50	1	2004-12-20 16:06				

Figure 8-30 Install Button

Step 3 In the resulting window, as shown in Figure 8-31, "Enter License Key," enter a License Key that you received on your *Right to Use* paperwork with your product.

Figure 8-31 Enter License Key

CISCO SYSTEMS				Home Shortcuts Account	Index Help About Logout
	IP Solution Ce	nter			
	Service Inventory	Service Design	Monitoring	Administration	User: admin
Security	Control Center Active U:	sers 🔹 User Access L	og 🔹		
You Are Here: • Administrati	on Control Center Licensing				Customer: None
	Install a License Ke	у			
Selection					
Hosts					
- Collection Zones					
• Licensing					
	License Key [*] :				
					Save Cancel
	Note: * - Required Field				Č

- Step 4 Click Save. Your newly installed license appears in an updated version of the Installed License table, as shown in Figure 8-30, "Install Button."
- Step 5 Repeat Step 2, Step 3, and Step 4 for each of the *Right to Use* documents shipped with your product.

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.

Note

Active Users

This section explains how to communicate with active users.

Navigate Administration > Active Users and follow these steps:

Step 1 After you navigate Administration > Active Users, a window that shows the currently logged users appears, as shown in Figure 8-32, "Active Users."

Figure 8-32 Active Users

CISCO SYSTEMS			Home Shortcut:	s Account Index Help About Logout							
սև սև	IP Solution Ce	IP Solution Center									
antillinaantillina -	Service Inventory	Service Design Moni	toring Administration	User: admin							
🔷 Security 🔹 C	ontrol Center 🔹 Active Us	e rs 🔸 U ser Access Log 🔹									
You Are Here: Administration	Active Users			Customer: None							
	Active Users										
	Show Active Users with User ID 🗾 Matching *										
				Showing 1 - 1 of 1 record							
	# 🔲 User ID	Host Name	Login Time	Last Access Time							
	1. 🥅 admin	smilley-ultra.cisco.com	9:48:48 PM PST 2/29/04	12:59:06 AM PST 3/1/04							
	Rows per page: All	-		[[<] <p></p>							
	Auto Refresh: 🔽			Disconnect							

Step 2 In Figure 8-32, if you have the privileges of SysAdmin or UserAdmin, you can disconnect one or more users. Select the check box next to each user you want to disconnect or select the check box in the header row, to select all the users. Then click the **Disconnect** button at the bottom of the window.



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.

Navigate Administration > User Access Log and follow these steps:

Step 1 After you navigate Administration > User Access Log, a window appears as shown in Figure 8-32, "Active Users."

ակել ակել	IP Solu	IP Solution Center								
additional diffication and	Service I	nventory Se	rvice Design	Monitoring Ad					User: adı	
🔷 Security 🔹	Control Center	Active Users 🤞	User Access Lo	g •						
e Here: • Administration	• User Access Log •	User Access Log							Customer: N	
	User Acce	ss Log Viewer								
election ser Access Log	Simple F	ilter 🔿 Advanced	Filter						Find	
ser Access Log	Fitter By:	Date	_		Matches:	×		_		
	r mor by:	10000			matorioo.				01-11-11-5-11-010-11-11	
	# Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Showing 1 - 5 of 4,043 record: Message	
	1.2004/03/01	01:54:15	admin	smilley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.	
	2. 2004/03/01	01:52:28	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.	
	3. 2004/03/01	01:35:23	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.	
	4. 2004/03/01	01:21:01	admin	smilley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.	
	5, 2004/03/01	00:44:11	back endadm		Logon	User	ERROR	SecurityActivity	Login failed.	

Figure 8-33 User Access Log Viewer with Simple Filter

All the log information about user actions appears.



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 8-34, "User Access Log Viewer with Advanced Filter," appears.

CISCO SYSTEMS	IP Soluti	Home Shortcuts Account Index Help About Logout							
millinaatilinaa	Service Inv	entory Se	rvice Design	Monitoring Ad	ministration				User: adm
🔷 Security 🔶 🤇	Control Center 🔹 A	Active Users 🔹	User Access Lo	g 🔹					
Are Here: Administration	User Access Log > Us	ser Access Log							Customer: No
	User Access	Log Viewer							
Selection User Access Log	C Simple Filte	r 🖲 Advanced	Filter						Find
	Date:	×				Action:	×	•	
	User Name:	н		_		Severity:	н	•	
	Host Name:	×				Activity:	×	•	
									Showing 1 - 5 of 4,043 records
	# Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
	1.2004/03/01	01:54:15	admin	smilley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.
	2. 2004/03/01	01:52:28	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.
	3. 2004/03/01	01:35:23	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.
	4. 2004/03/01	01:21:01	admin	smilley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.
	5. 2004/03/01	00:44:11	backendadm		Logon	User	ERROR	SecurityActivity	Login failed.
	Rows per pa	age: 5 💌						144	Go to page: 1 of 809 💿 🕽 🕅

Figure 8-34 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**.



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

Step 7 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 Daemon (rvd) after installation. The changes being made here only affect Java WebStart applications, such as Inventory Manager and the topology tool.

95362

Navigate Administration > Manage TIBCO Rendezvous and follow these steps:

Step 1 After you navigate Administration > Manage TIBCO Rendezvous, a window appears as shown in Figure 8-35, "TIBCO Rendezvous."



TIB/Rende	zvous		[efgh-ultra]
Agent for Java – 7.	1.3		
			2003-06-18 22:50:06
State:		Component Information	
information	component:	rva	
Configuration:	version: license ticket:	7.1.3 65599	
change state	host name: IP address:	efgh-ultra 128.107.128.130	
security	client port:	7600	
connection	http tunnel:	enabled on main port	
subjects	state: total clients:	running	
<u>http tunnel</u> certificates	direct clients:	0	
certificates	tunnel clients:	ŏ	
Miscellaneous:			
<u>copyright</u>			
web home			

- Step 2 From Figure 8-35, 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 8-35.
- Step 3 In Figure 8-35, when you click **connection**, a window such as Figure 8-36, "Connection Configuration," appears.

Figure 8-36 Connection Configuration

Connection Configuration						
Accept Client Connections on Listen Port: 7600						
TIB/Rendezvous	Daemon Connection:					
service:	7530					
network:						
daemon:						
Submit Reset]	95361				

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 rvd port number from the existing value, change the service field to your new rvd port number for ISC. Then click Submit. Then Figure 8-36 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."

- In Figure 8-35, click change state, follow the instructions, and you complete this functionality. Step 4
- Step 5 From a terminal window, change to the bin directory of your ISC installation, such as /opt/isc-3.2/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 Inventory Manager or the topology tool, these changes are in effect.

