Cisco Service Portal Configuration Guide

Release 9.3.1
January, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Service Portal Configuration Guide
© 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Organization Design 1-1

Overview 1-1

Accessing Organization Designer 1-1

Organization Designer Home Page 1-1

Navigation 1-2

Search 1-3

Maintaining Organizational Entities 1-4

Organizational Entities and their Relationships 1-7

Directory Integration and Organizational Entities 1-7

Organizational Units 1-8

Maintaining Organizational Units 1-8

Configuring Organizational Units 1-9

Groups 1-15

Configuring Groups 1-15

Using Groups in Service Design 1-17

Queues 1-18

Tips for Working with Queues 1-19

Configuring Queues 1-19

People 1-22

Configuring People 1-23

Functional Positions 1-28

Creating a New Functional Position 1-29

Modifying a Functional Position 1-30

Deleting a Functional Position 1-30

Roles 1-30

Role Hierarchy 1-30

Searching for Roles 1-34

About Object-Level Permissions 1-35

Roles with Object-Level Permissions 1-37

Capabilities 1-38

Custom Roles 1-43

Sample Custom Roles 1-46

Authorizations 1-48

Setting Up an Authorization Structure 1-48

CHAPTER 2 **User Profiles** 2-1

Overview 2-1

Information 2-1

Preferred Language 2-2

Calendar 2-3

Preferences 2-3

CHAPTER 3 **Site Administration** 3-1

Overview 3-1

Administration Home 3-1

Directory Integration 3-2

Site-Wide Authorizations 3-2

Email Templates 3-2

Viewing Email Templates 3-3

Configuring Templates 3-3

Using Namespaces 3-4

Demand Center Templates 3-4

Lists 3-5

Business Goals and Initiatives 3-6

Language 3-7

Offering Attributes 3-7

Site Settings 3-8

Customizations 3-8

Common Settings 3-10

My Services Settings 3-13

Demand Center Settings 3-17

Web Services Setting 3-17

Custom Styles 3-17

The Person Popup 3-19

Entity Homes 3-20

Debugging Settings 3-21

Data Source Registry 3-22

Support Utilities 3-23

Log and Destination Folder Settings 3-23

View and Download Files 3-25

Adjusting the Panel Displays 3-27

CHAPTER 4 **Custom Style Sheets** 4-1

Overview 4-1

Custom Style Sheets 4-2

Overview 4-2

Prerequisites 4-2

Customizing Built-in Modules 4-2

Customizing User-defined Portals 4-3

Defining a Custom Style 4-3

Turning On Custom Style Sheets and Headers/Footers 4-4

Modifying Customizations with Browser Cache Enabled 4-5

Customizing Styles 4-5

Preserving Customizations 4-11

Known Errors and Omissions 4-12

Unknown Errors and Omissions 4-12

Upgrading from Previous Versions 4-12

Style Summary and Recommended Practices 4-13

Style Summary – Built-in Modules 4-13

Style Summary – User-defined Modules 4-18

Recommended Practices 4-19

Example Screenshot, and What Each Style Specifically Affects 4-19

Custom Headers and Footers 4-20

Overview 4-20

Procedure 4-20

Customizing Page Headers and Footers 4-21

CHAPTER 5 **System Administration** 5-1

Overview 5-1

Intended Audience 5-1

Terminology 5-2

Startup and Shutdown Procedures 5-2

JBoss 5-2

WebSphere 5-2

WebLogic 5-3

Restarting Cognos Server 5-3

Ongoing Infrastructure Maintenance Tasks 5-3

Backup Methodology 5-3

Application Server Tuning 5-4

Database Tuning 5-6

Managing the Application 5-10
The Basics 5-10
Key Configuration Files 5-10
Managing Logs 5-11
Administering ColdFusion 5-13
Data Sources 5-15
Creating "Backing Tables" for External Dictionaries 5-16
Applying Maintenance Releases and Patches 5-17
Configuring Service Export via SSL or NTLM 5-17
Request Center Cached Data 5-18
Application Security 5-19
Reporting and Advanced Reporting 5-20
Escalation Manager 5-21
Service Manager 5-21
Relationship Manager 5-22
Service Portal Installation 5-22
Multicast Settings 5-23
Performing Application Housekeeping 5-24
Requistion Purge 5-24
Workflow Purge 5-27
Service Link Messages Purge 5-29
Manage Integrations 5-30
Integration Types 5-30
Directory Integration 5-31
Single Sign-On 5-33
Interactive Service Forms (ISF) 5-33
Active Form Rules 5-33
Service Link 5-34
Including Custom Content during Installation 5-34
Overview 5-34
How the Installer Works 5-34
Including Custom Content during Installation 5-34
Catalog Deployer and Configuration Management 5-37
Recommended Process for Copying a Database 5-37
Installing Additional Service Link Adapters 5-38
Overview 5-38
Installing Additional Service Link Adapters 5-38
Configuring SSL for Service Link Inbound Documents 5-39
Overview 5-39

Creating a Certificate Keystore 5-40
Installing the Keystore for the Application Server 5-41
Configuring SSL for Service Link Outbound Documents 5-58
Overview 5-58
Outbound URL 5-59
Importing the Signer Certificate to a Trusted CA Keystore 5-59
Troubleshooting 5-66
Commonly Monitored Traces and WebSphere Tracing 5-67
Limiting Outbound Email 5-67
Recreating Missing Service Link Messages 5-69
Environment/Platform Overview 5-69
When to Call the Cisco Technical Assistance Center (TAC) 5-69
Errors 5-72
Error Log Locations 5-72
Error Conditions and Error Codes 5-73
Sample Environment Matrix 5-81

CHAPTER 1

Organization Design

- Overview, page 1-1
- Organizational Units, page 1-8
- Groups, page 1-15
- Queues, page 1-18
- People, page 1-22
- Functional Positions, page 1-28
- Roles, page 1-30
- Authorizations, page 1-48

Overview

Organization Designer is the primary tool for structuring your service organization. In this module, you set up and maintain the following components of a Cisco Service Portal (Service Portal) implementation:

- Organizational Units
- Groups
- Queues
- People
- Functional Positions
- Roles

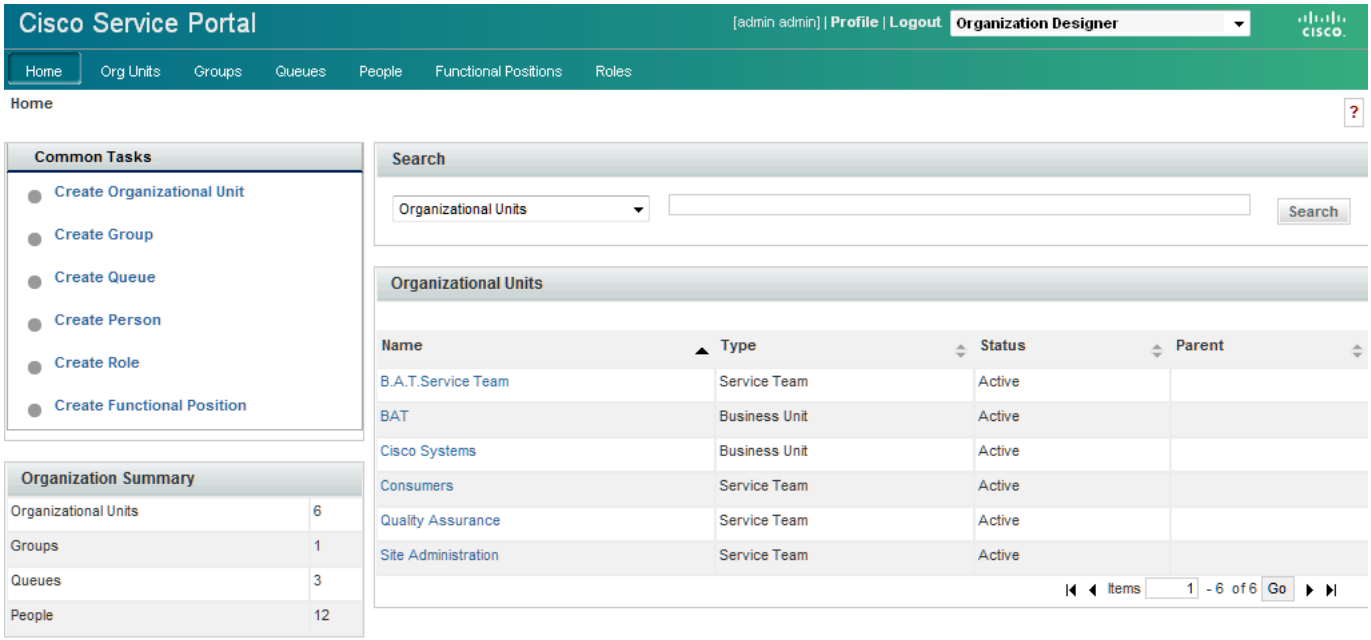
Accessing Organization Designer

The Organization Designer module is available with all installations of Service Portal. It appears in the module drop-down menu for all users who have been granted the capability to use Organization Designer.

Organization Designer Home Page

The Organization Designer Home page is divided into the following areas.

- The **Navigation** pane shows the options available in this module, as well as the current page. As you navigate through various options, a trail of "breadcrumbs" is left (starting from the Home page), so you can easily return to any page you previously visited.
- The **Common Tasks** pane groups the most frequently used tasks into one location, primarily to make the creation of new entities easier. Entities can also be created by clicking the **Add** button available on the component-specific page.
- The **Organization Summary** pane displays the number of entries for organizational units, groups, people, and queues.
- The **Content** pane allows you to search for an organizational entity, create a new entity, or modify an existing entity.

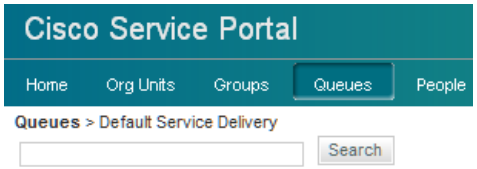


Navigation

The navigation bar, located at the top of the browser window, enables you to quickly navigate from one Organization Designer component to another, or return to the Organization Designer Home page.

Each time you view a particular organizational unit, group, person, queue, or role, a navigation trail displays what you are viewing, and within what component, in Organization Designer. This trail is created in the top of your browser window, and makes it easy for you to know where you are and where you have been in Organization Designer.

Here is an example of a breadcrumb trail, which uses a *[component] > [name of the object you are viewing]* format:



Another way to navigate to a different component of Organization Designer is to use the Home page search, described below. Once you search for a particular entity type and select an entity of that type, control will be transferred to the corresponding component.

Search

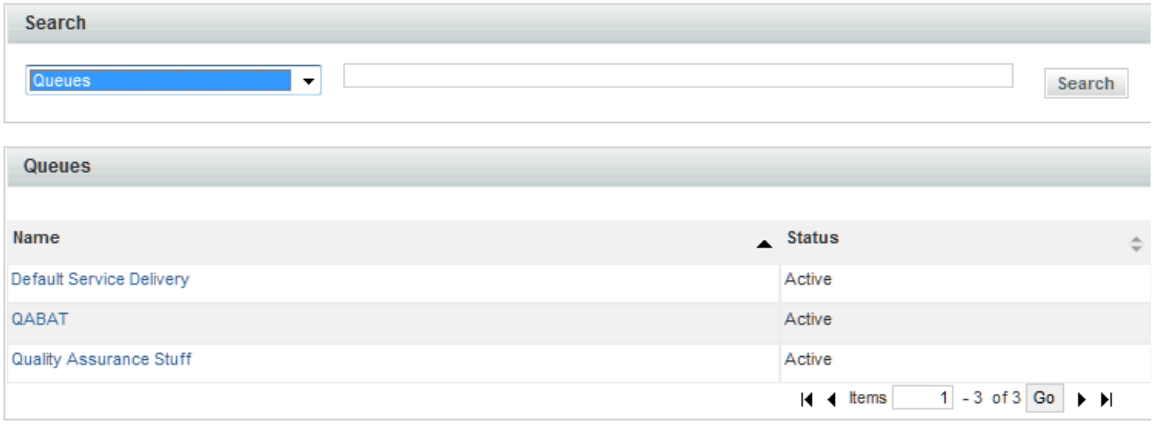
Organization Designer offers two search methods to help navigate and locate different organizational components.

- Home page search
- Component-specific search

Home Page Search

The Home page allows you to conduct a simple search for different components in one location. Use the **Search** area on the Home page to quickly locate an entity by type and optionally by name as well.

- Start by selecting the entity type to display. Once you have made your selection all entities of the specified type will be shown in the content pane, below the search box. Search results display in alphabetical order.



- You can browse the list of entities displayed in the content pane. As you move the mouse over each entity name, a hyperlink appears. You can click on that link to go to the Organization Designer page where you can view or modify details of the entity definition.

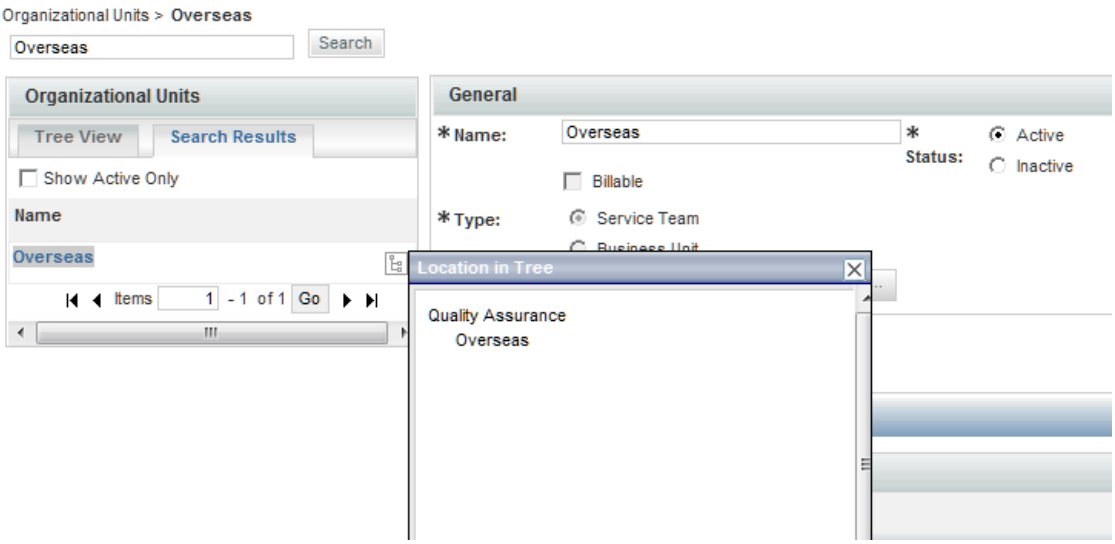
- To narrow the list of entities displayed, select then entity type, then enter all or part of the entity name in the text field, and click **Search**. All objects that meet the search criteria are displayed— for example, entities whose names match a complete or full word entered. You can then browse those entities and select one for a more detailed view.

Component-Specific Search

Component-specific searches allow you to view search results within the specific component, without having to go back to the Home page. This allows you to remain within the component, and continue your work, without having to navigate away.

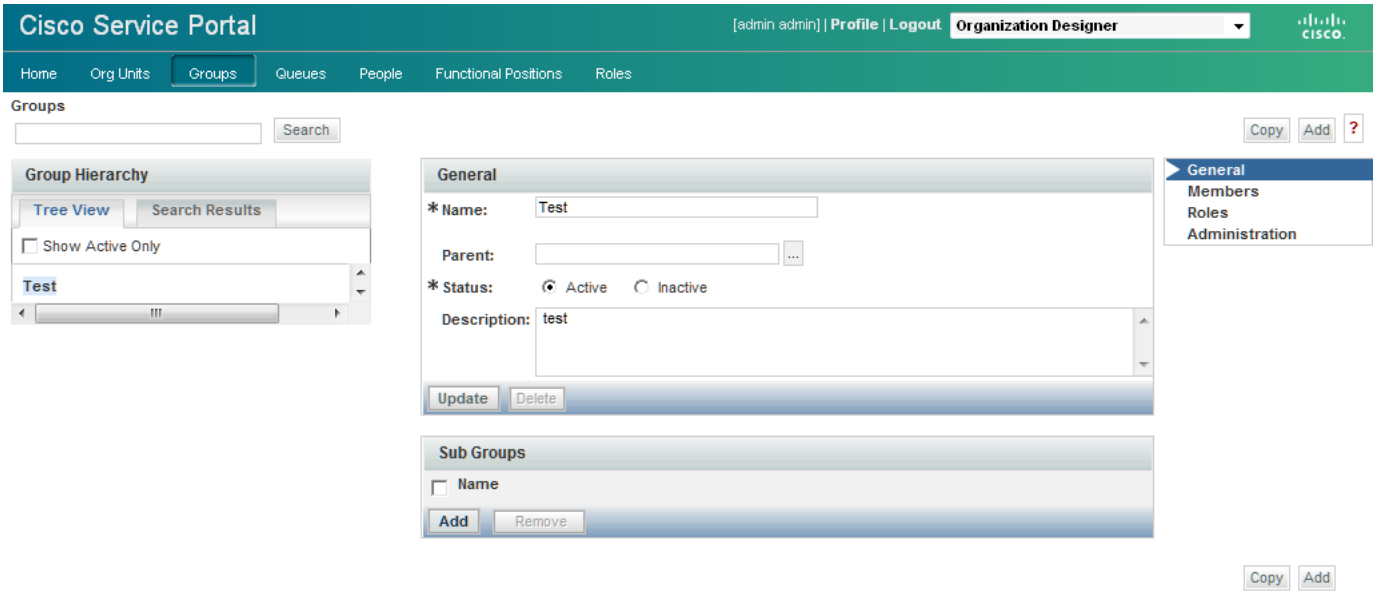
You can conduct a component-specific search for any entity managed by Organization Designer.

Those entities with hierarchical structures, for example organizational units or roles, also allow you to view the hierarchy. Simply click next to the search result.



Maintaining Organizational Entities

Each type of organizational entity has its own home page, accessible by clicking the corresponding tab from the Organization Designer home page or by searching for and then selecting an entity of the corresponding type. The home page displays the “General” properties of the entity. Additional pages are listed to the right of the content pane, as shown in the sample Group below. These pages may vary according to the type of entity.

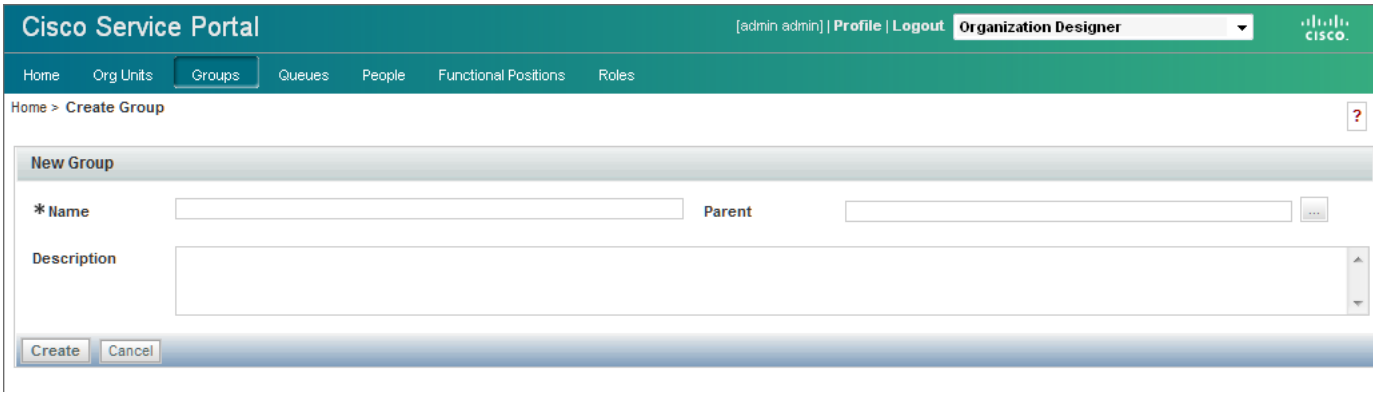


Creating an Entity

There are two ways to create an entity through Organization Designer:

- Click the **Create** link from the Common Tasks page of the Organization Designer home page.
- Click the tab in the navigation pane corresponding to the type of entity to be created. Once the entity's home page is displayed, click **Add**.

In either case, a create page for the selected entity type appears.



That page typically includes all of the required attributes for creating the entity. Once you supply data for these attributes and click **Create**, the entity will be created. The standard set of pages is then available, to allow you to maintain additional aspects of the entity definition.

Copying an Existing Entity

You can copy an organizational entity as a means of cloning that entity. Copying an entity copies all of the properties of the entity, including its members, except those properties that uniquely identify the identity, such as the organization name or a person's name and login ID.

To copy an entity, display its definition and click the **Copy** button on the General page. You then assign it a new name and save the entity. All pages of the new entity definition are then available for edit.

Deactivating an Entity

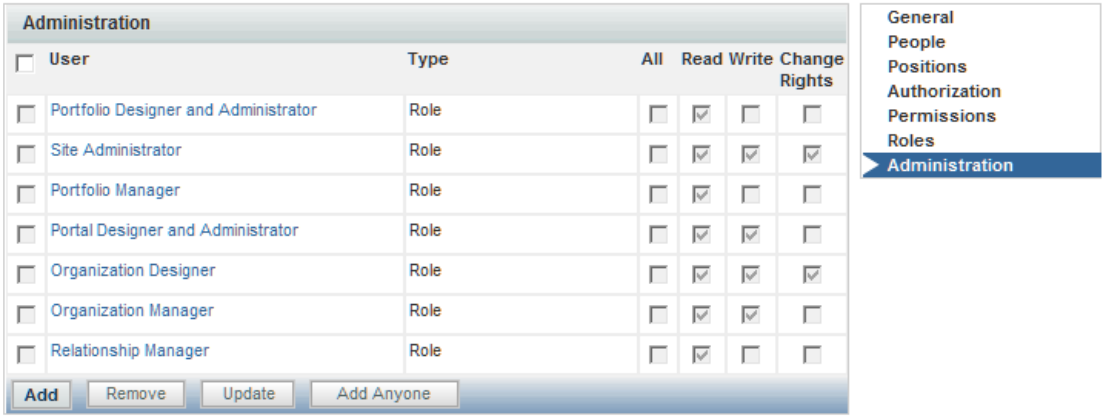
Organization Designer allows you to "hide" an entity from view within other modules, such as Service Manager or Service Designer, without deleting it from the system. An inactive entity will not be displayed in any Search windows. For example, when a service designer attempts to assign a task to a particular queue, only active queues are displayed. When you change the status of the entity, you will be asked to confirm this change.

Deleting an Entity

You can delete an entity only if it is not active and in use. For example, you cannot delete a queue which is used in a delivery plan. You must first deactivate the queue before you can delete it.

Administration

All organizational entities have an Administration page. The Administration portion of an entity allows you to specify who can view or edit the records created for the entity.



Administrative rights on an entity may be assigned to a specified organizational unit (hence inherited by all people in that OU), functional position, queue, group, or role. In addition, rights may be assigned to "Anyone", which means just that—any user who has the capability of accessing Organization Designer would be able to modify information on that entity. "Anyone" should be added sparingly, if at all.

The following rights may be assigned:

Right	Description
All	User has permission to read (view information), write (modify and update information) and Change Rights (change read/write access) this entity.

Read	User has permission to only view information for the entity, but cannot modify information.
Write	User has permission to view and modify information for this entity.
Change Rights	User has the ability to change the read/write access for the entity. Permissions are "grayed out" when the user does not have permission to change the rights.

System-defined entities are automatically granted pre-determined sets of administrative rights. These entities are grayed out, and cannot be deleted or modified. However, additional organizational units, people, roles, groups, or functional positions can be assigned administrative rights.

Organizational Entities and their Relationships

Understanding how organizational entities are related is critical to setting up a well functioning implementation. For example:

- Every user must be represented as a **Person**, viewable and maintainable via Organization Designer.
- All **People** must belong to at least one **Organization**. To be able to request services, people belong to a Business Unit (a type of organization). People who perform service delivery tasks also belong to one or more Service Teams.
- **People** and **Organizations** are granted **Roles**, which determine which modules they will be able to access, and what capabilities they will have within each module. Granting a role to an organization ensures that all members of that organization inherit that role. For example, people who work for the same business unit can typically order the same set of services.
- In addition to Organizations, ad-hoc **Groups** of **People** can be set up. The Groups can then be assigned **Roles**. For example, perhaps one or two people on several service teams, not the entire team, should be able to run Request Center reports and create custom reports. Setting up a group makes it easier to ensure that the proper set of people has the proper capabilities.

The dependencies between entities influence the ways you can work with these entities in Organization Designer. The sections on the individual entity types explain these dependencies in more detail.

Directory Integration and Organizational Entities

In principle, the following organizational entities can be created and refreshed via directory integration:

- People, including their membership in roles, groups, and organizations
- Organizations, including both business units (departments or divisions of the company whose members are allowed to order services) and service teams (those company employees who perform tasks within Request Center)

In many installations, business units are automatically created as part of Directory Integration. This is logical, since the business unit corresponds to a real-life division of a corporate entity, and should be part of most enterprise-based directories. Users of Organization Designer can freely create additional business units, for example, for testing purposes or modify aspects of the organizational unit not maintained via the directory integration.

Although directory integration capabilities support automatically creating service teams, this is less common. A service team may be completely a Service Portal artifact, created so that a customized set of people are authorized to work on specific tasks. Therefore, the enterprise outside of the Service Portal need have no knowledge of such an organization, and it would be the responsibility of administrators to create and maintain such a service team/business unit.

Similarly, directory integration allows the assignment of roles and groups to people to be imported into Service Portal from the directory. However, the directory in many cases does not hold such information, since roles and groups are typically Service Portal artifacts, created expressly to facilitate usage of Service Portal, and with no applicability to other enterprise activities. Therefore, users of Organization Designer will typically have to maintain both the role definition and the assignment of the role to people, as well as to organizations and groups.

Organizational Units

An organizational unit, or OU, represents the organizational structure of your company.

Maintaining Organizational Units

There are two types of organizational units:

- Service teams, comprised of people who deliver services
- Business units, comprised of people who request and receive services

Organizational units can contain members of the unit, or people, and can be linked with queues. In fact, when adding a new person to the system, you are required to select a default, or Home, organizational unit.

Service Teams

Service teams deliver the services requested. Service teams are linked to queues created in Organization Designer as well as service groups created in Service Designer. While service teams consist of the people who deliver services, or service performers, service groups represent both the teams and the system processes for service delivery. Service teams can “own” the group of services, and thus be responsible for managing the work related to delivering those services.

A service performer can belong to one or more service team OUs. It is recommended that you create service teams based on skill sets of your performers.

Business Units

Business units have as members those people who request and receive services. Only business units are billable, and appear in My Services in Bill To fields when placing a request for a service. Therefore business units are often organized based on a company's cost center structure.

Though a service performer can belong to many service teams, it is recommended that you assign a business unit as the person's Home organizational unit, rather than a service team. Because only business units are billable, assigning business units as the Home OU allows for proper tracking of costs and charges when performers request services for themselves.

Note Every user must be assigned to one "Home" Organizational Unit (OU). Users may be assigned additional Organizational Units but only one can be set as "Home".

Maintaining an Organizational Unit

Once you create an organizational unit, the organizational unit will be available for modification and entry of additional data as outlined below.

Page	Description
General	General information about the organizational unit, including sub organizational units assigned to a parent OU.
People	Members of the organizational unit, including both people and queues.
Position	People and queues assigned to functional positions specified for organizations.
Authorization	Authorization and review structure for the organizational unit.
Permissions	Entities with permission to order on behalf of the organizational unit, or manage the service team.
Roles	Roles currently assigned to the organizational unit.
Administration	Entities with permission to view and/or modify organizational unit information within Organization Designer.

Deactivating Organizational Units

If directory integration is in place and is configured to refresh people and organizations, you must also ensure that the organizational unit to be deactivated is not associated with any valid, active user in the enterprise directory. If that user were to log in, the organizational unit would be re-activated. Also, deactivating an organizational unit does not deactivate any queues associated with that organizational unit.

Configuring Organizational Units

The General page of an organizational unit allows you to edit information provided when creating the OU. You can make the unit active or inactive, as well as further develop the hierarchical structure by adding or removing sub organizational units.

General information about an organizational unit is summarized below.

Name	Name of the organizational unit
Status	Active or Inactive.
Billable	Check if service performers can bill for work time to complete requests for the business unit. This option is available only for business units.
Type	Click either Service Team or Business Unit.
Parent	Click ... to search for and select a parent organizational unit.
Language	The displayed language for the organizational unit.
Description	Any text describing the organizational unit.

Organizational Unit Hierarchies

Service Portal allows you to create a hierarchical structure of parent and child organizational units. Each organizational unit can have a parent OU and one or more child, or sub, OUs.

Organization unit structure has the following effects:

- Statistics (such as SLA compliance or the volume of tasks or requests processed) can be consolidated for a parent OU, for accounting or reporting purposes, within the Advanced Reporting modules.
- Different styles (governing the appearance of the screens) can be associated with parent or child organizational units, allowing designers to customize the user experience.
- Sub-organizational units can inherit roles and permissions from the parent, facilitating the assignment of responsibilities.

Sub organizational units, and therefore the members of that sub OU, inherit all the roles and permissions assigned to its parent organizational unit. Because of this inheritance rule, you must make sure you set up role-based access carefully. An example would be using a bottom-up approach, in which the lowest child Organizational Unit is assigned the greatest number of roles, and therefore greatest responsibilities, and the higher up the parent Organizational Unit, the fewer roles are assigned.

Because you are adding sub organizational units to a parent, a helpful way to order your work is to:

1. Create the sub-organizational units.
2. Create the parent organizational units.
3. Add the sub organizational units to the parent OU.

OU Members

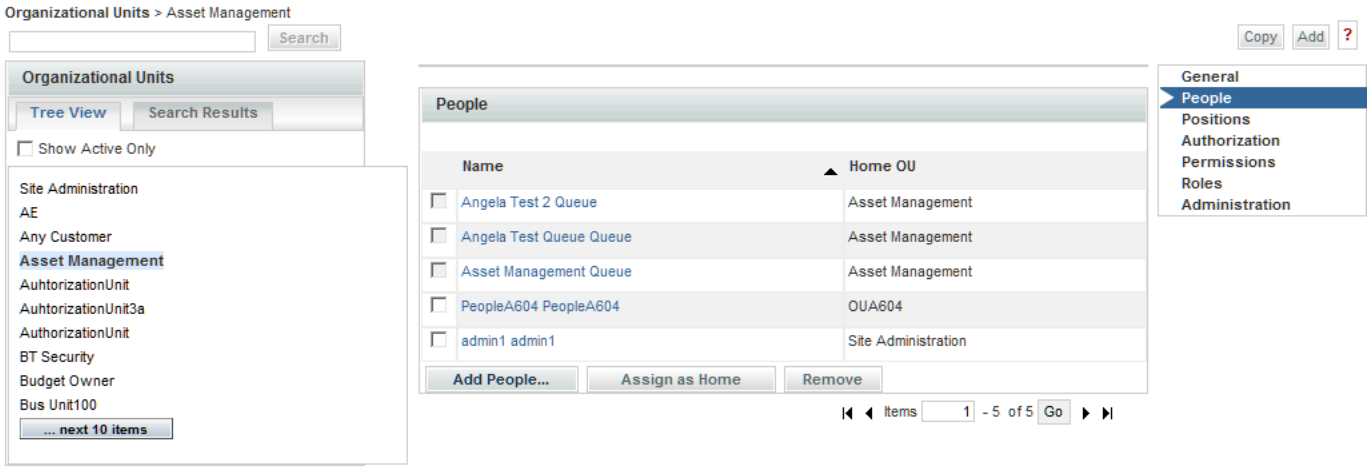
You can specify the people who belong to an organizational unit. A person may be assigned to multiple OUs, but must have one Home OU. The process of associating an organizational unit with a person consists of the following:

1. Create the organizational unit.
2. Create the person.
3. Associate the person with the organizational unit – There are two ways you can create a person/OU relationship:
   - Assign a person to an organizational unit – Adding a person via the Org Units page of the People component allows you to assign multiple people to an OU.
   - Assign OU(s) to a person – Adding an organizational unit via the Members page of the People component allows you to assign multiple OUs to a particular person at once.

For service teams, you can specify which queues the team is responsible for. The process of associating an organizational unit with a person consists of the following:

1. Create the service team organizational unit.
2. Create the queue – When you create a service team, you need to create a queue for the service team to receive work. Before you can assign a queue to an organizational unit, you must first create the queue.
3. Associate the queue with the organizational unit – There are two ways you can create a queue/OU relationship:

- Assign a queue to an organizational unit – Adding a queue within organizational unit information allows you to assign multiple queues to an OU.
- Assign OU(s) to a queue – Adding an organizational unit within a person's information allows you to assign multiple OUs to a particular person all at once.



The box to the left of the queue/person's name will be grayed out if the current organization is home for that entity. You cannot remove a person who has the OU assigned as the Home OU. If you wish to remove the person from the OU, you must first reassign a new Home OU for the person by maintaining the Person entry. You can then remove the person as a member of the non-home OU.

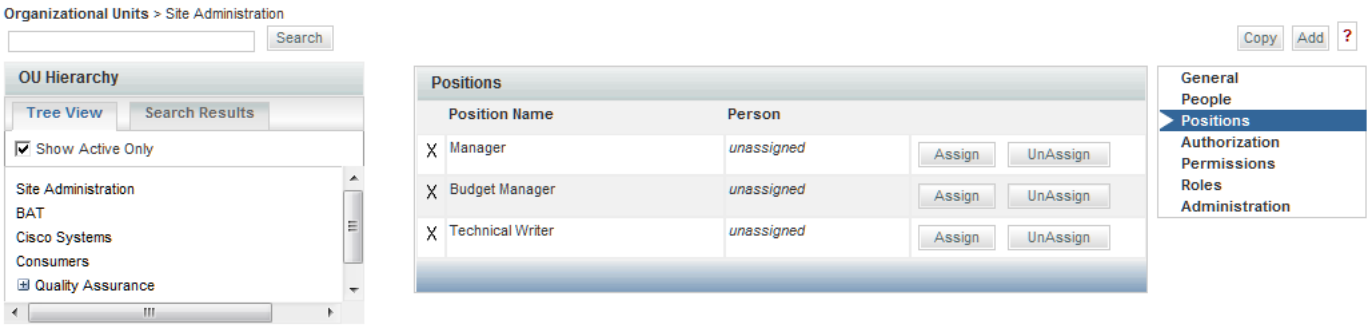
To change the home affiliation for the entity, click the box to the left of the queue/person name, then click Assign as Home. To change the entity home affiliation once it has been established, you will need to go to the Organizations page of Person or Queue component of Organization Designer.

Functional Positions

Any queue or person that is associated with an organizational unit may be assigned to any functional position for the organization. Before you can assign an entity to a functional position, the functional position must exist. Organization Designer has several pre-defined functional positions, or you can create a functional position and relate it to organizational units.

The order for creating a functional position/assigned person relationship is:

1. If necessary, create a new functional position.
2. If necessary, create the organizational unit.
3. On the Positions page of the Organizational unit, assign an entity (person or queue) who is a member of that organization unit to fill the position.



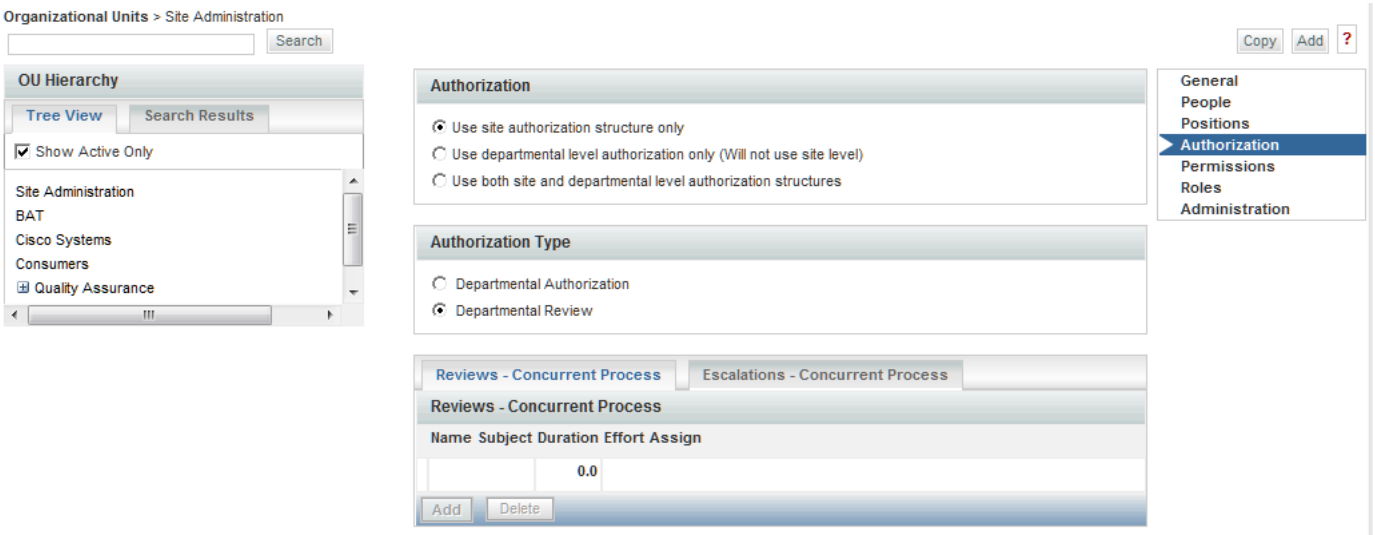
An "X" to the left of a position name indicates that the position has not been filled.

To assign a person or queue to a functional position, click the **Assign** button. A pop-up window is displayed allowing you to search for and select the person or queue to be assigned.

An entity can be removed from a functional position by clicking the **Unassign** button. If the functional position is responsible for performing tasks or performing other duties, functional positions should not be left unfilled.

Organization-Level Authorization

You use Organization Designer to establish the authorization structure for an organizational unit, that is "Departmental Authorization" and "Departmental Review". Configuration abilities are similar to those available at the site level and at the service group level. They are described in the section of this document on Authorizations.



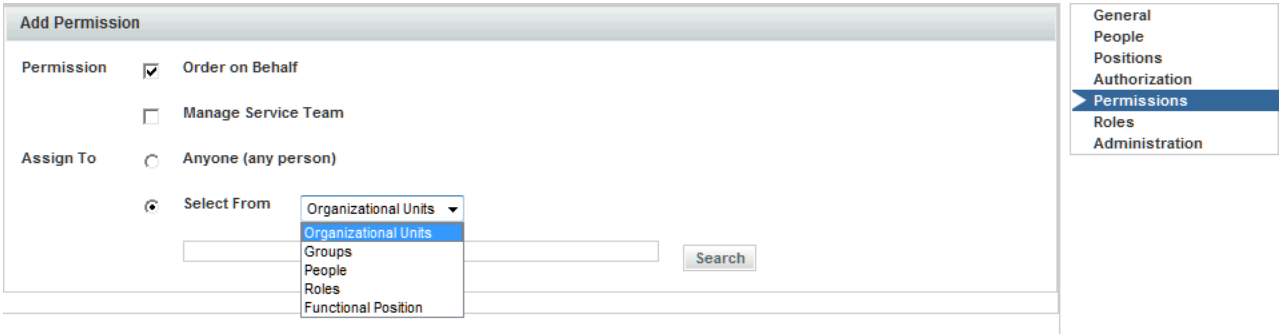
Permissions

Permissions allow you to control which entities have permission to do something to the organizational unit. You can set up the following permissions:

- Order on Behalf – Designates who can order on behalf of other members of a Business Unit OU using My Services.

- Manage Service Team – Designates who can view a Service Team OU in the navigation pane's tree view in Service Manager.

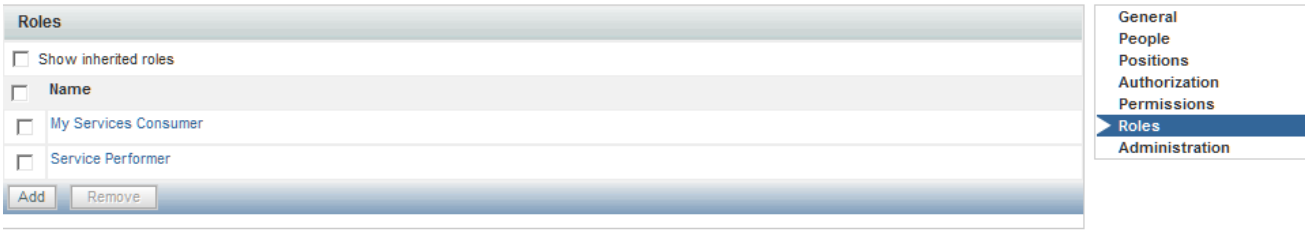
To assign permissions for an OU, click **Add Permission** to display the Add Permission window. You then indicate which permission(s) to add, and the entity to which it should be added.



In general, it is more efficient and more easily maintainable to grant permissions to an organizational unit, group, or role rather than to individual people.

Roles

All members of the organizational unit inherit the roles assigned to the organizational unit. In addition, sub organizational units inherit roles from their parent organizational unit.



The **Show inherited roles** option allows you to choose whether to show those roles inherited from a parent organizational unit. If not selected, only roles directly assigned to the organizational unit display.

When an organization is created, it is automatically granted the My Services Consumer role. This allows any members of the organization (or sub-organizations) to access My Services and to order any services for which they have been granted ordering permission. (Permission to order a service is granted via the service or service group.)

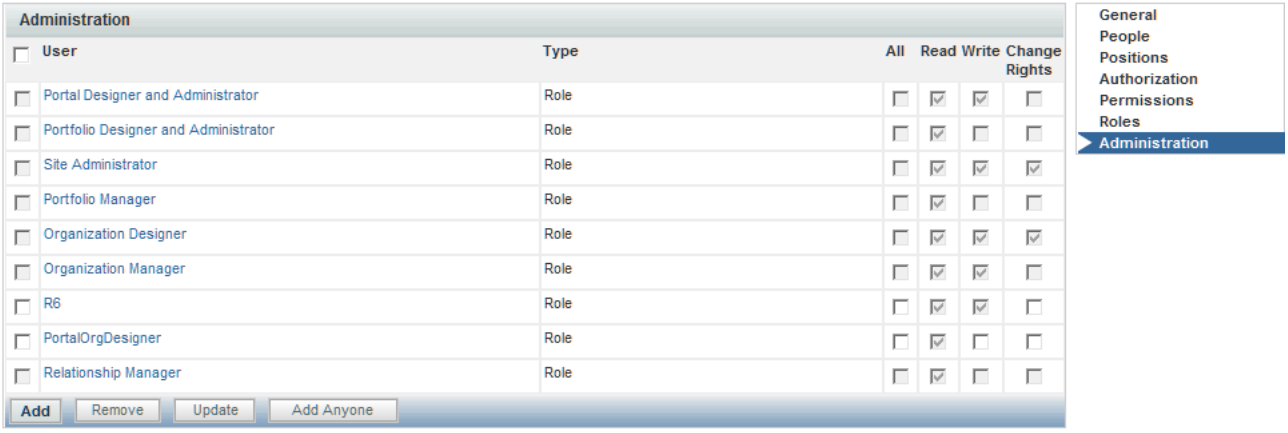
Any role defined in Request Center—both default roles provided by Service Portal and custom roles created in each installation—can be granted to an organization. For a detailed description of available roles and how to create a custom role, please see the section of this document on Roles.

Users should typically not change aspects of the organization's definition that are refreshed via directory integration. If a change is needed, it must be applied to the contents of the directory that is the source of the data.

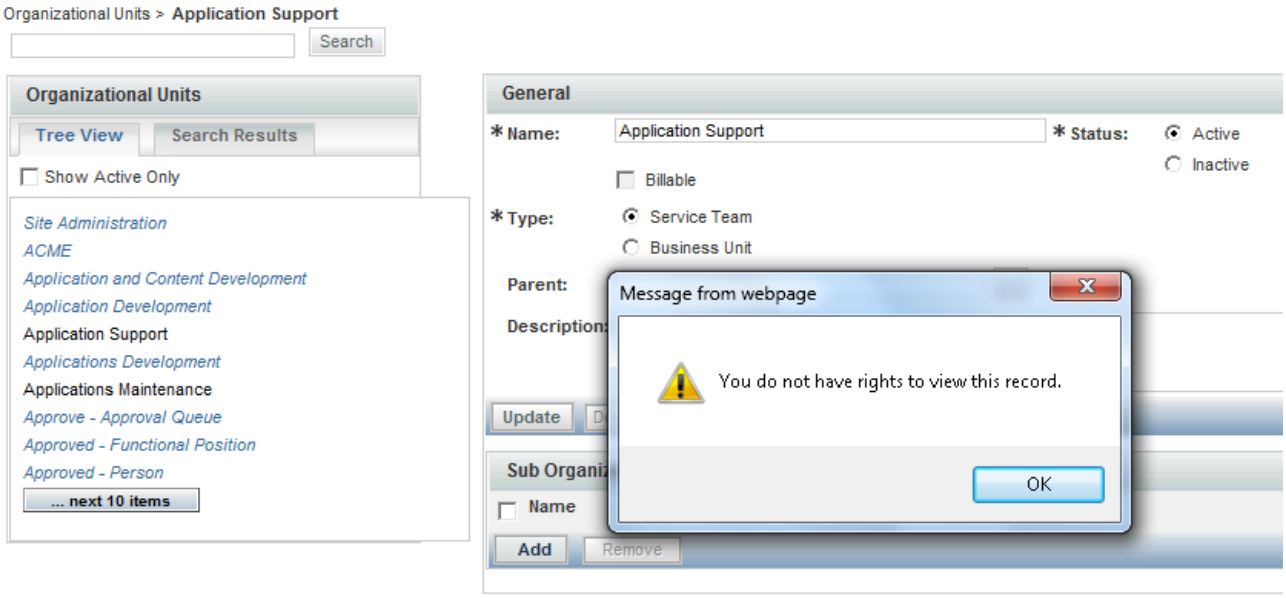
Any administrative privileges allowing changes to organizations are overridden by entity protections that are applied to an entity at any non-home sites. Please see the *Cisco Service Portal Designer Guide* for more information on setting entity protection levels.

Administration

The Administration options show the permissions granted to users to read, write, or change rights for the current organization and allows administrators to assign these permissions to custom roles. The prebuilt roles grant the associated permissions to all organizations; adding a custom role or a specific person, OU or position, allows you to assign permission to read and/or write organizational data at the object level, that is, on an organization by organization basis.



Organization Designer does not "hide" selected OUs or queues using permissions, but prevents a user from reading or modifying a particular OU or queue. Entities that a user is not permitted to read or write are then indicated by italics, and will present a popup if that user tries to access that entity:



You can either do this directly on the Administration page for the specific entity, or you could do this:

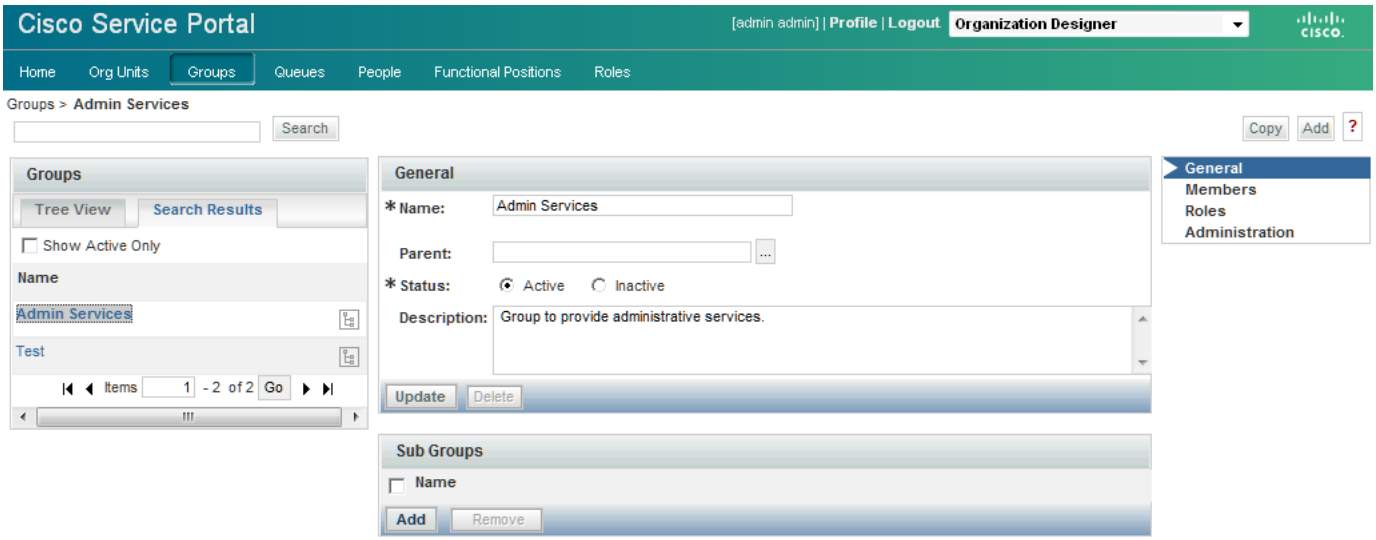
1. Create a role with the Access Organizational Unit Configuration and Access Queues Configuration capabilities.
2. Go to the Permissions page for the role.

3. Set the Read/Write permissions for the role using the wizard as follows:
   a. OUs: *All Service Teams of which user is a member*
   b. Queues: *All queues associated with service teams of which user is a member*

Groups

A group is an organizational and management tool to enhance your ability to organize services, allocate costs, assign permissions, and grant access rights at your site. Groups allow you to consolidate OUs and/or people with some shared characteristics into a single entity. Roles can then be assigned to a group, rather than to multiple organizations or people.

A group can have multiple subgroups. The subgroups inherit the members and roles assigned to the parent group.



Configuring Groups

Group configuration includes the following pages.

Page	Description
General	General information about the group
Members	Organizational units and people who are members of the group
Roles	Roles assigned to the group
Administration	Access control within Organization Designer

Configuring General Group Information

The General portion of group information allows you to edit information provided when creating the group. You can make the group active or inactive, as well as further develop the hierarchical structure by adding or removing sub groups.

Adding or Removing Sub Groups

Sub groups allow you to create a hierarchical structure of parent and child groups. Each group can have both a parent group and one or more child, or sub, groups. Sub groups are grouped within a parent group.

Sub groups, and therefore the members of that sub group, inherit all the roles and permissions assigned to its parent group. Because of this inheritance rule, you must make sure you set up your role and permission system carefully. An example would be using a bottom-to-up approach, in which the lowest child group is assigned the greatest amount of roles, and therefore greatest responsibilities, and the higher up the parent group, the fewer roles assigned to it.

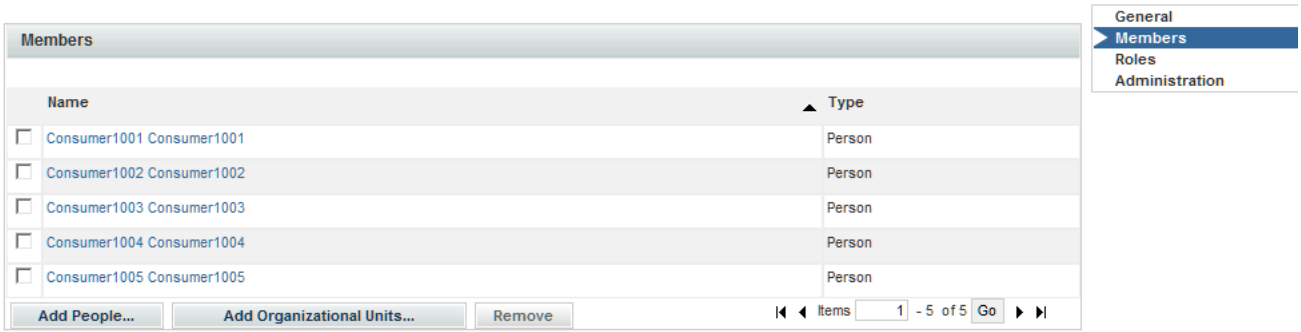
Because you are adding sub groups to a parent, a helpful way to order your work is to:

1. Create the sub groups.
2. Create the parent groups.
3. Add the sub group(s) to the parent group.

Members

Group members consist of a combination of organizational units and/or individual people. You can specify the people and organizational units that belong to the group. The process of associating a group with a person or OU consists of the following:

1. Create the group.
2. Create the person or organizational unit—before you can assign a person or OU to a group, you must first create the person or create the OU within the system.
3. Associate the person or OU with the group.



A member may be removed from the group at any time by clicking the box to the right of the member name and then clicking the **Remove** button.

Roles

When assigning roles to a group, all members of the group inherit the role. In addition, sub groups inherit roles from their parent group. The **Show inherited roles** option allows you to choose whether to show those roles inherited from a parent group. If not selected, only roles directly assigned to the group display.

Before you can assign a role to a group, you must first make sure the role exists. Service Portal provides several pre-configured roles for your use, or you can create a new role to fit your company needs.

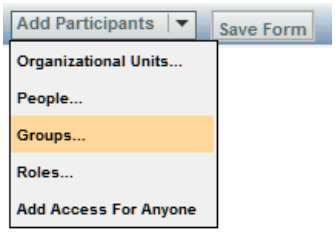
Using Groups in Service Design

Permissions can be assigned to groups, rather than being assigned to individual people or to organizations. It's a way to group disparate people or organizations and give them the same permissions.

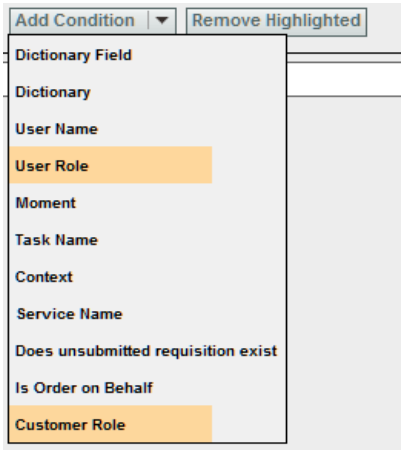
Within Service Designer, a Group can be used *directly* when granting object-level permissions related to service groups, services and form groups. Those object-level permissions are:

Object	Permission
Service Group	Design services and change data in this service group
Service Group	View services and other information in this service group
Service Group	Order service group services
Service Group	Assign rights
Service	Order service
Active Form Group	View forms
Active Form Group	Design forms

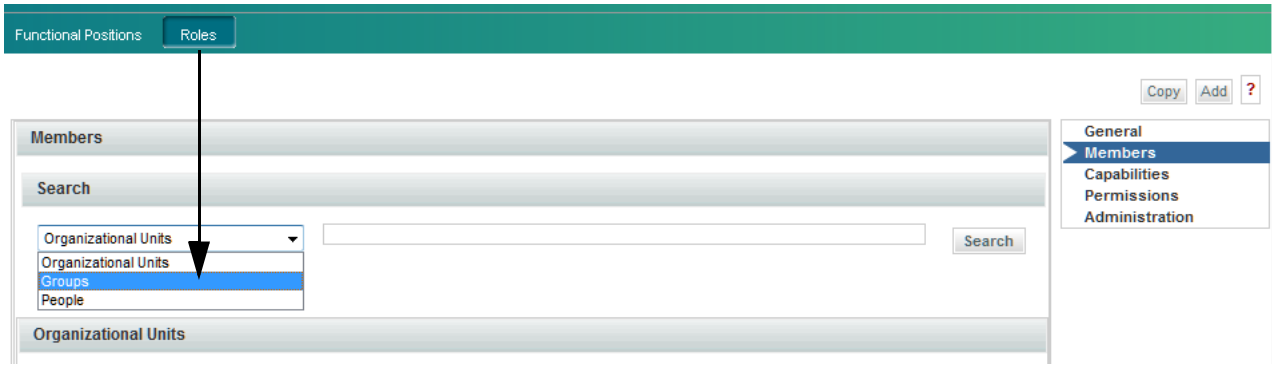
Groups can also be used as an Additional Participant when assigning Access Control for dictionaries.



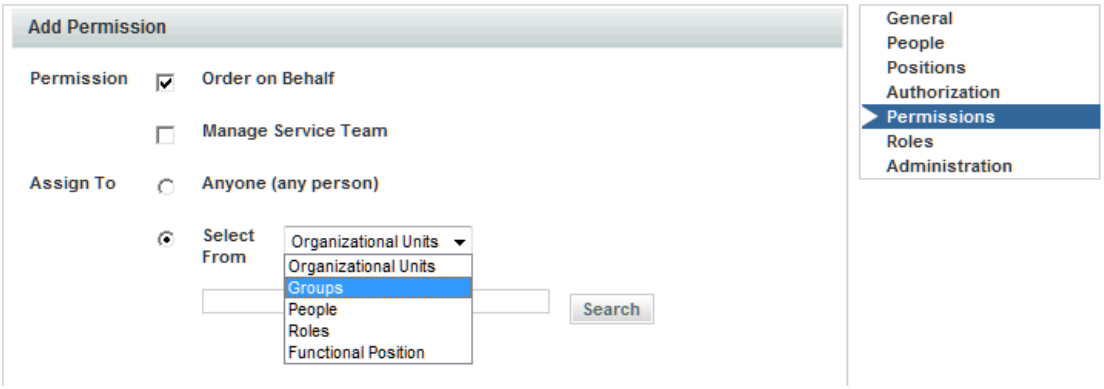
In addition, because a group can be a member of a role, you can also use groups *indirectly* wherever you can use a role. For instance, conditional rules include a User Role and Customer Role condition type. In this case, you could create a group, make it a member of a role, and use it in defining conditions for conditional rules.



Within Organization Designer, anyplace where you are working with roles, you can use a group to collect together the people/OUs to whom you with to grant that role.



Finally, when assigning object-level permissions for OUs and people in Organization Designer, you can also use a group.



Queues

A queue is a repository, or "Inbox," for tasks that need to be performed. Work is assigned to queues so that tasks are not dependent on any one individual.

After creating a queue, you use the Access Queue object-level permission to specify who can access the tasks sent to the queue. People are not "members" of a queue. They simply staff a queue by having permission to access it. Anyone with access to the queue can perform the tasks assigned to the queue. Members of the service team that is the Home OU for a queue automatically receive the Access Queue permission.

Service Portal comes with one pre-configured queue—the Default Service Delivery Queue. If a task is not assigned to a task performer, or if a namespace used to dynamically assign a task does not evaluate to a valid queue, the task will be placed in the Default Service Delivery Queue.

Defining a queue consists of entering the information on the Queue pages summarized below.

Page	Description
General	General information about the queue
Org Units	Organizational units assigned to the queue
Contact	Contact phone number(s) and email address

Calendar	Work hours and days, as well as holidays
Permissions	Assign who has permission to access queue information within Service Manager
Administration	Entities with permission to view and/or modify queue information within Organization Designer

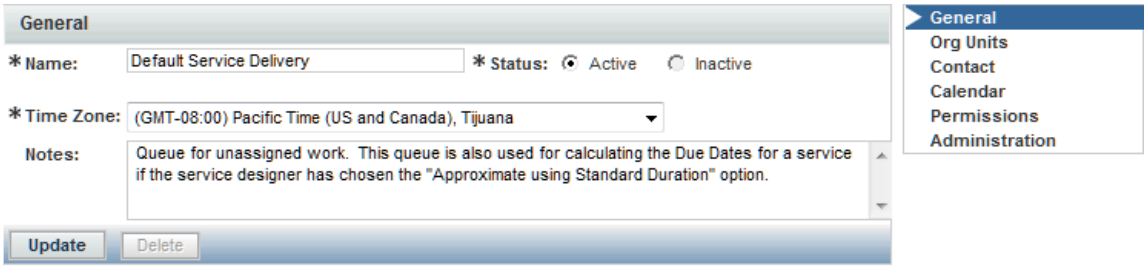
Tips for Working with Queues

- Queues are mapped to service teams. Only use service teams as the Home OU for queues.
- Every service delivery task should be mapped to a queue for execution of tasks.
- Ensure that queue calendars and time zones are set correctly. Request Center calculates due dates and times for tasks based on the calendar and time zone settings of queues to which the tasks are assigned.

Configuring Queues

Configuring General Queue Information

The General page of a queue allows you to edit information provided when creating the queue. You can deem the queue active or inactive, as well as set the time zone for the queue.



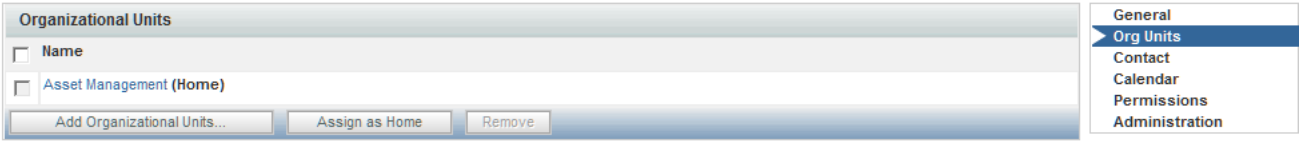
The queue's general properties are summarized below.

Name	Name of the new queue. The name may be identical to the name of the service team (organizational unit) is the Home OU for the queue. When the queue name is displayed, it will have “Queue” appended to the specified name. The maximum length of a queue name is 100 characters. The name can contain alphanumeric characters and the underscore; it should not contain special characters such as the ampersand (&).
Time Zone	Time zone for the queue's primary location. The queue time zone, as well as calendar, is critical for estimating the due dates of tasks assigned to the queue.
Notes	Any text describing the queue.

Queue Organizational Units

You can specify the service team(s) assigned to a queue. When you create a new queue, you must assign a default, or Home, organizational unit. Though several service team OUs can be responsible for a queue, a queue can only have one Home OU. To make an association between an organizational units and queue, use one of the following methods:

- Open the service team information and assign queues.
- Open the queue and assign service teams.

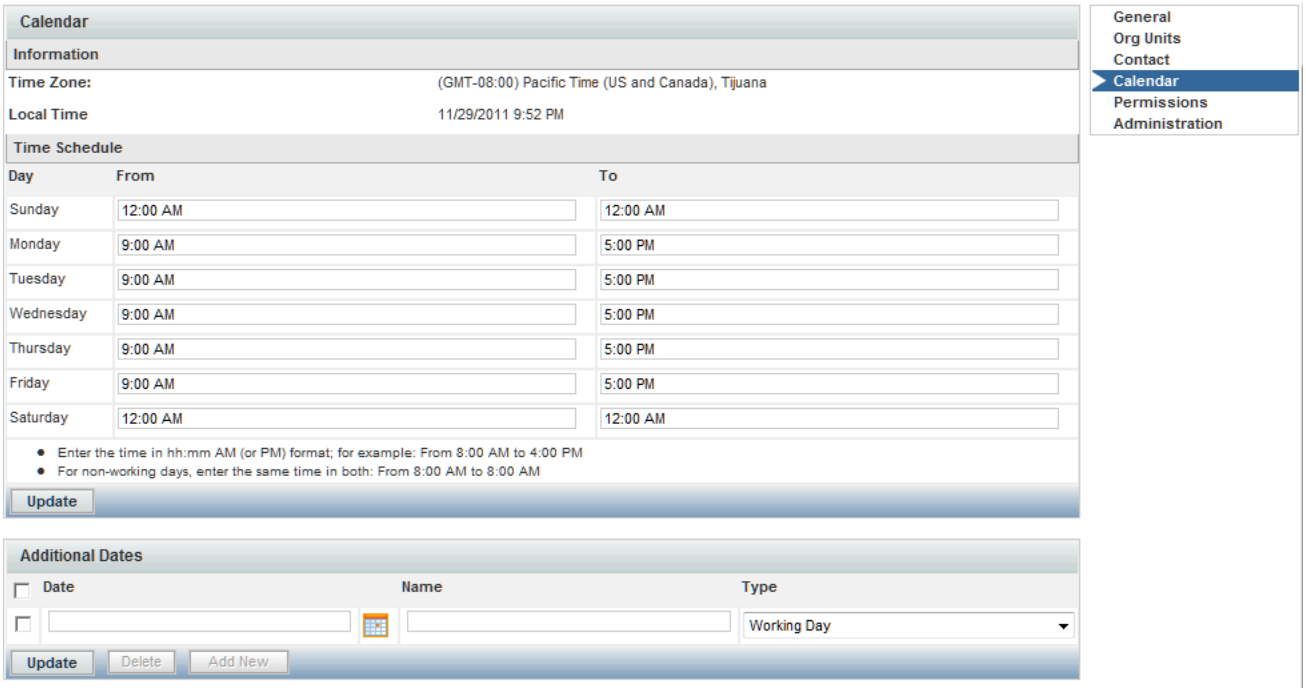


Queue Contact

Administrators may refer to the queue contact information if a problem arises with delivery of tasks assigned to a particular queue. Different contact types (email, phone numbers) are provided. Multiple email addresses can be accommodated for the Email field in Queue Contact. The email addresses need to be delimited by a semi-colon, for example, jdoe@company.com;dsmith@company.com.

Queue Calendar

Use the Calendar page to set the work hours and days, and assign non-work days and holidays. Calendar information is used to compute due dates for tasks and services according to the queue's work hours.



For a new queue, the work schedule defaults to five days a week, from 8am to 6pm, in the time zone specified for the queue (specified on the General page), as shown in the "Time Schedule" portion of the Calendar page. You may make any necessary changes to the work hours.

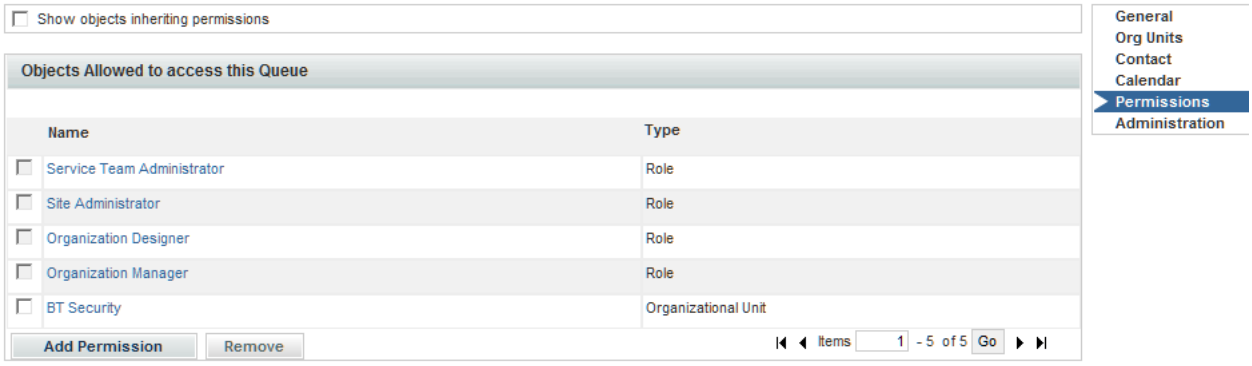
- Type times for the From and To fields, using a HH:MM AM/PM format.
- Type the same time in both the From and To fields, for example 12:00 AM and 12:00 AM, to designate days that you do not work.
- Click **Update** to save changes.

You can use the "Additional Dates" portion of the Calendar page to tag a specific day as either a holiday or working day. Select **Add New** to add a new date. Enter the date by selecting from the calendar icon ( ), specify a Name for the date (for internal documentation), designate the Type as either a Holiday or Working Day, and then click **Update**. These additional dates will also be taken into account when computing task and service due dates.

Queue Permissions

Permissions allow you to control who or what has permission to access the queue. Accessing the queue allows the user to see and perform tasks for a particular queue within Service Manager.

By default, some pre-configured roles automatically can access any queue. Consequently, any entity (person, organization, or group) granted one of those roles will be able to access the queue. In addition, members of any OUs associated with the queue automatically are allowed to access the queue.



People

People are all the individuals who either receive services via My Services or provide services via Service Manager, as well as all the administrators, managers, and users of all other application modules.

You must set up all individuals who are system users, whether they are within or external to your organization. The following two statements are important to remember:

- A person is a member of one or more Organizational Units.
- A person can only be “Home” in one OU.

Creating New People

Service Portal provides three mechanisms for adding people:

- Organization Designer allows administrators to create a person interactively, using the pages described in this section.
- The Import Person event in Directory Integration can create a person and his/her home OU. For more information, see the *Cisco Service Portal Integration Guide*.
- The Directory Task available in the service’s workflow (delivery plan) can create a person based on service form data. For more information, see the *Cisco Service Portal Designer Guide*.

No matter how a person is created, their personnel information can be maintained using Organization Designer.

When creating a new person, you must assign a default, or Home, organizational unit to the person. Therefore make sure you create the organizational unit before you create the new person.

To add a new person the following fields are required.

First Name	First name of the person.
Last Name	Last name of the person.
Email	Contact email address.
Time Zone	The time zone associated with the person's primary address. If not provided, the default server time zone is used.
Language	The language displayed on the user interface for the person. If not provided, English is used.

Home OU	The person's default organizational unit. It is recommended that you select a business unit as a person's Home OU, rather than a service team.
Login	A unique login identifier.
Password	A password used to log on to the system. If using Organization Designer, retype the password to confirm. Any character in the character set supported by the application can be used in the password.

Configuring People

The following pages allow you to configure information about people:

Page	Description
General	General information about the person.
Org Units	Organizational units to which the person belongs.
Address	Company and/or personal address information.
Contact	Contact phone number(s) and email address.
Extensions	Extended information about a person.
Calendar	Work hours and days, as well as holidays.
Permissions	Entities with permission to order on behalf of the person, or assign an authorization delegate.
Roles	Roles available to the person.
Administration	Entities with permission to view and/or modify information about a particular person within Organization Designer.

General Person Information

The General page of a person's information allows you to edit the following information.

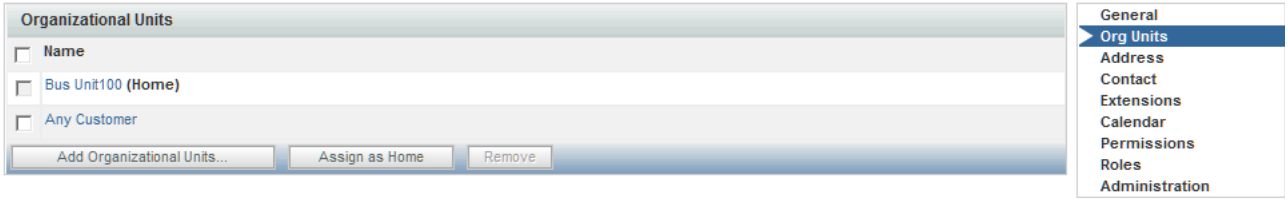
Title	Abbreviation used when addressing correspondence to the person; Ms. or Mr., for example.
First Name	First name of the person.
Last Name	Last name of the person.
Status	Active or Inactive.
SSN	Social security number.
Birth Date	Date of birth.
Hire Date	Person's hire date.
Time Zone	The time zone associated with the person's primary address. This is used to calculate and display the proper due dates for tasks and services according to the person's time zone.
Language	The language displayed on the user interface for the person.
Employee Code	Company-derived employee code, if any.
Supervisor	The supervisor for the employee. This is used in “supervisor” tasks such as certain authorizations. You use Service Designer to create these tasks.

Notes	Any additional descriptive information about the person.
Login	A unique login identifier.
Password	The password used to log on to the system.
Confirm Password	Retype the password.

Assigning Organizational Units to People

When you create a person, you must assign a default, or Home, organizational unit to the person. Though a person can have only one Home OU, they can be a member of several organizational units. To make an organizational units and people association, use one of the following methods:

- Open the organizational unit and assign people.
- Open the Org Units page of an individual person's information and assign organizational units to the person.



These methods are functionally equivalent, so select whichever one is more convenient.

In addition, people may be assigned to organizational units via the Org Units attribute mapping in Directory Integration.

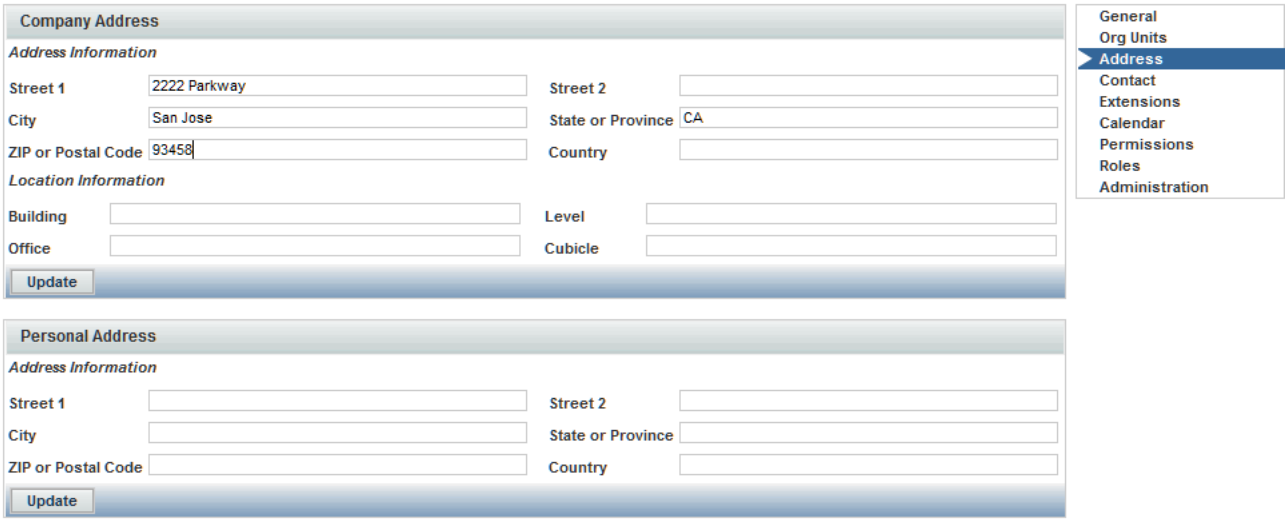
Assigning an organization as the person's home OU automatically removes the home OU designation from the previous home.

Address Information

You can enter company and personal addresses, as well as specific location information, for each person.

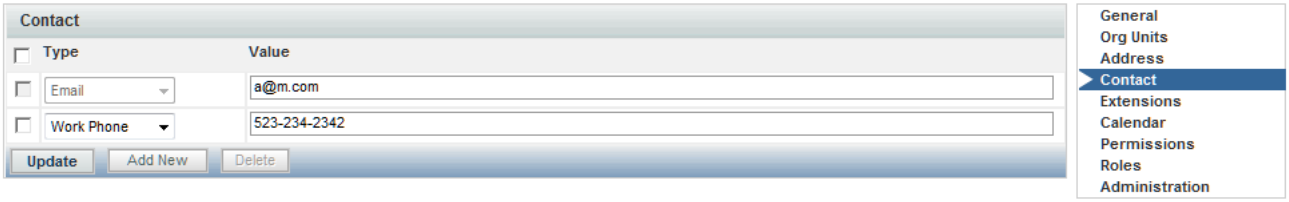
Having valid address information for a person may be critical to ensure:

- Task performers can find the person when a service needs to be performed in person, for example, changing the hardware configuration of a workstation
- Delivery plans can use expressions that are dynamically evaluated to route work to a queue that serves the area where the service requestor is located. Such “location-based queues” are common in geographical distributed organizations.



Contact Information

You can enter multiple means of contacting a person, each one identified by a contact type, such as telephone, fax, or pager number.



- The email address specified when you create a person displays as the first contact. You can change this email address, but you cannot delete it—it is indicated with a “grayed out” check box.
- All contact types except email address can be freely added to and deleted from the person's contact information.

Extensions

The main reason for extensions is to load LDAP attributes into “extensions to the person record” so that conditional workflow can be driven from these attributes. Extensions allow you to add additional information about a person. This information can be tailored to your company's business and financial codes and structure. For example, you can enter a person's department and cost center numbers or names. In addition, you can upload a person's picture, which is displayed whenever viewing a person's profile information, such as in a search.

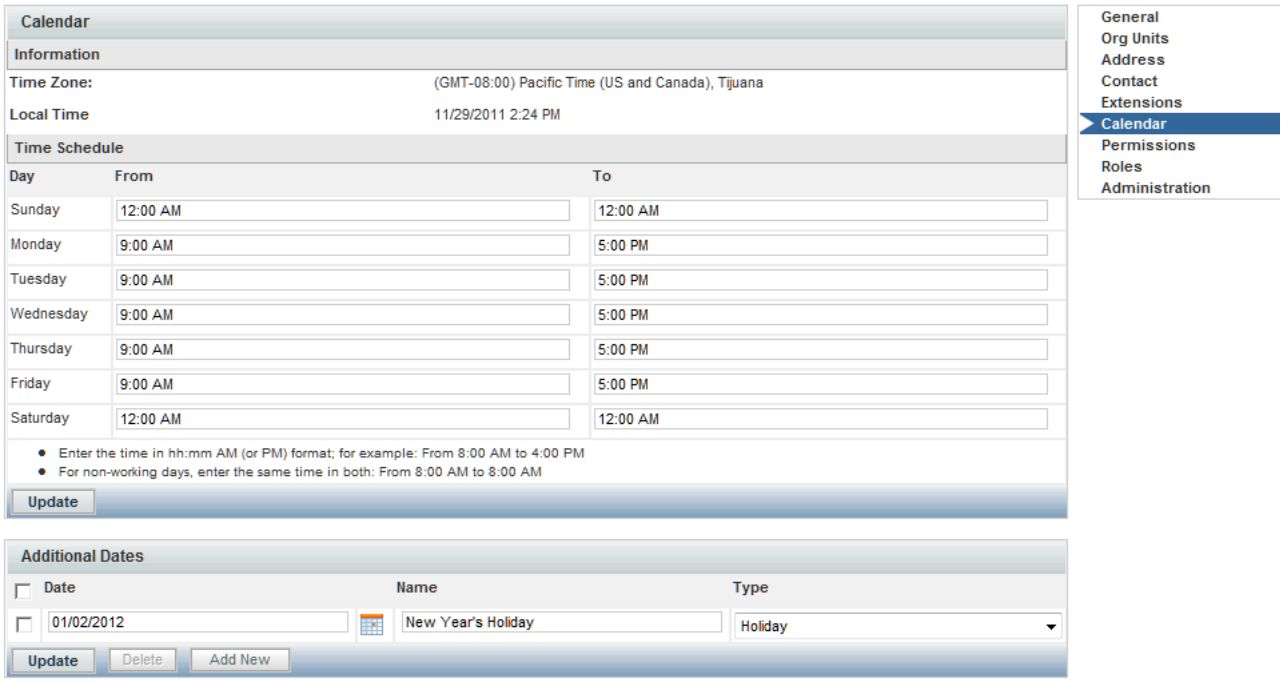
Most of the fields on the person profile are used in application processing, and the mapping should ensure that source attribute(s) provide a value appropriate for the field; that is, do not try to overload these fields with more information than would be suggested by the field name, or with information that does not match the field name.

Service Portal also includes fields which provide an extension to the standard personnel data. These fields appear on the Extensions page of the Person information. Some of the most frequently required extended fields have been assigned meaningful names (such as Company Code and Division), but others have the names Custom 1 through Custom 10, and are intended to be freely used, with no pre-conceived semantics. If you have additional personnel information in the LDAP directory that needs to be exposed in Request Center, map the attributes containing that information to one of the personnel extended fields.

You cannot change “Custom” to another field name. However, if these fields are included in a service form, a label can be assigned which correctly reflects the field contents.

Configuring a Person's Calendar

Calendar information sets a person's availability. You can enter a person's work schedule, detailing the hours of work for each day of the week. In addition, you can specify holidays and other days in which the person is not available. For service group members, this information is used to compute the work hours spent on a task and to determine whether the task was delivered on time or late.



The local time and time zone reflects the time zone assigned to the person in the General page.

Make any necessary changes to the work hours.

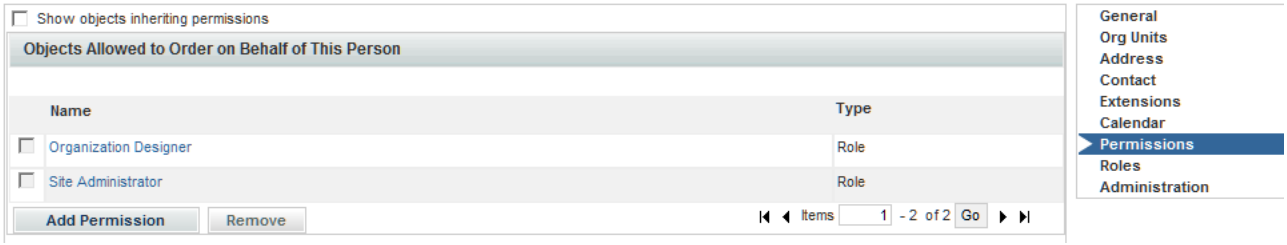
- For Time Schedule, type times for the From and To fields, using a HH:MM AM/PM format.
- Type the same time in both the From and To fields, for example 12:00 AM, to designate days that are not workdays.

If a holiday falls on a day of the week that is normally a work day, specify that date as an “Additional Date”, with a Type of “Holiday”. Conversely, if a work day falls on a day of the week that is usually not a work day, specify that date as an “Additional Date” and assign a Type of “Working Day”.

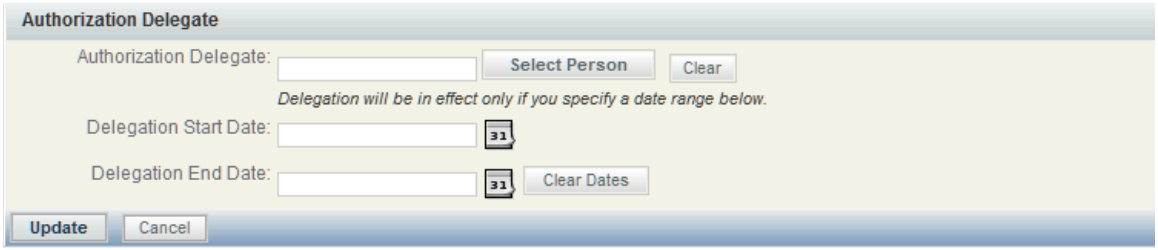
A person can access his/her own calendar via the Profile option that appears alongside the module menu.

Assigning Permissions to a Person

Permissions define an object's capability to affect a chosen person. These objects can be organizational units, groups, other people, roles, and functional positions. For people, you can set up permissions to define who can order on behalf of the selected person:



The Permissions page also designates the Authorization Delegate for the selected person in the event that an authorizer cannot fulfill authorization duties, for example if the authorizer is on vacation. The delegate can perform authorizations for the person during the time period specified using the Delegation Start Date and Delegation End Date fields.



A person may assign their own Authorization Delegate using the Preferences page of the Profile option. Since delegates may be designated many times, for different periods, it is recommended that individuals be responsible for designating their own delegates, rather than using Organization Designer to do this.

To assign a person's Authorization Delegate supply the information summarized below.

Authorization Delegate	Click **Select Person** to search for and select the person responsible for authorizations in the event that the original authorizer is unavailable.
Delegate Start Date	Type a start date, using a MM/DD/YYYY format, for the delegate to take over authorization responsibilities. You can also click 31 to select a start date from a calendar.
Delegate End Date	Type an end date, using a MM/DD/YYYY format, for the delegate to end authorization responsibilities. You can also click 31 to select an end date from a calendar.

If you are using the delegation functionality, you should keep in mind:

- The delegate does not automatically receive notification for an upcoming authorization. To notify the delegate, the appropriate namespace (#Alternate…#) must be used in the To: field of the email. If no delegation is in effect, the namespace value will be blank in the notification.
- Once the delegate clicks an action button (Approve, Reject, or OK) for the delegated approval task, they become its owner—ownership of that task is actually transferred to the user who clicks the action button.
- After this ownership transfer, the original approver's ability to "see" the task will be determined by their role and by OU membership. In order to see the completed approval task (in My Services), the original approver would need to have the My Services Professional role (or at least a role with the "View Authorizations for My Units" capability) and would need to be in the same OU as the person who actually performed the approval.

Assigning Roles to a Person

There are two ways to create a person/role relationship:

- Assign role(s) to a person – Adding a role within a person's information allows you to assign multiple roles to a particular person at one time.
- Assign a person to a role – Adding a person within role information allows you to assign multiple people to a role. See Assigning People to a Role.

Deactivating a Person

If directory integration is in place and is configured to refresh people and organizations, or to perform a Single Sign-On, you must also ensure that the person to be deactivated is not longer an active user in the enterprise directory. If that user were to log in, the person entry would be re-activated.

Deleting a Person

Once a person has performed any activities within Service Portal, the person entry cannot be deleted. The person can be made Inactive to prevent them from logging on or performing further activities.

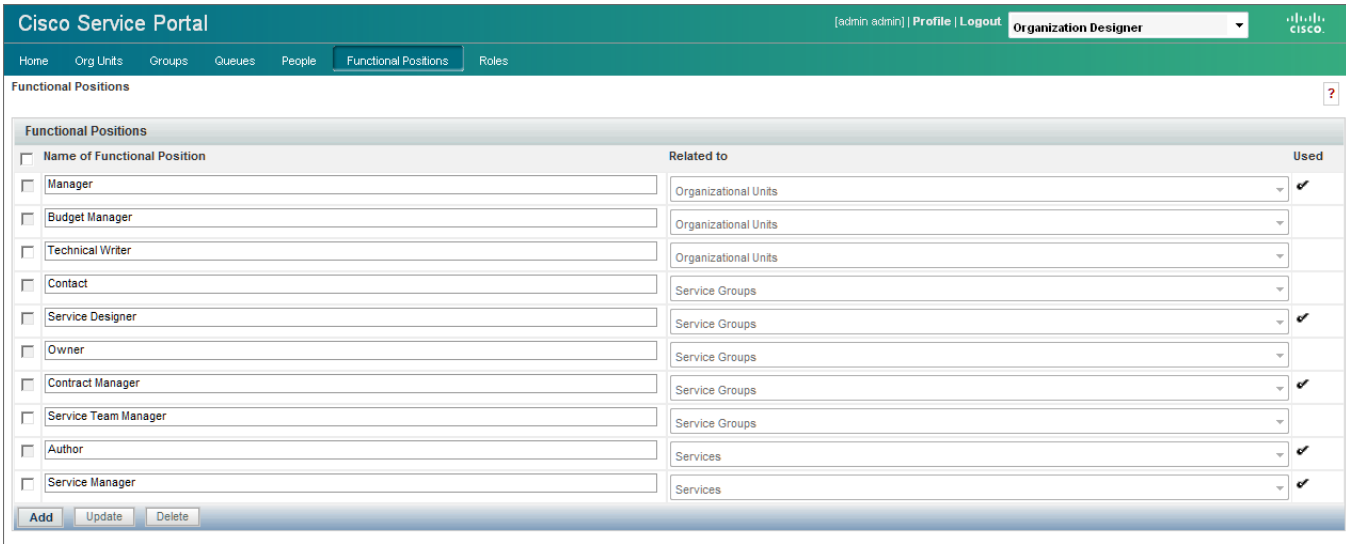
Functional Positions

Functional positions can add flexibility to configuring a service's delivery plan and assigning responsibilities for various aspects of the Service Portal application. A task within the system can be assigned to a functional position. A people, queue or role can then be assigned to fill that functional position. The functional position can be referenced in tasks (assigned as a task performer) or in namespaces (included in an email sent to the appropriate person or people.)

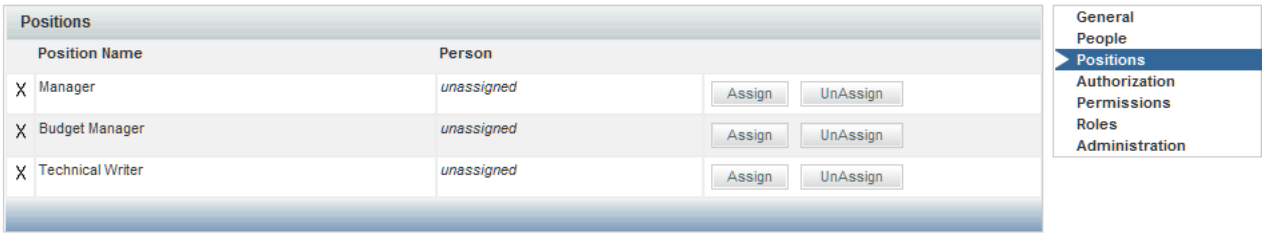
Functional positions can be associated with one of three entity types:

- Organizational units
- Service groups
- Services

Service Portal provides several standard functional positions, which cannot be modified. In the illustration below, the checkbox to the left of the system-defined functional positions is grayed out, indicating that these positions cannot be deleted or updated. The "Queue Approver" position was created at this site.



Functional positions associated with each type of entity will be displayed on the Organization Designer or Service Designer page for maintaining the corresponding entity type. For example, with just the standard functional positions associated with an organization, the Positions page for maintaining Organizations would look like this:



Creating a New Functional Position

If the system-defined functional positions do not meet your company's requirements, you can create new functional positions. Click the **Add** button on the Functional Position page—a new line will appear at the bottom of the list of positions:

The name assigned to the functional position should not contain spaces, even though this is permitted. A name with embedded spaces cannot be used as a namespace variable. By selecting the “Type”, you associate the position with an organizational unit, service group, or service.

Modifying a Functional Position

When attempting to update a functional position, keep in mind:

- The standard positions display a disabled (“grayed out”) check box next to the position name and cannot be deleted, even if they are not in use.
- You can only update a created functional position's name.
- You cannot update a position's association. If you need to change an association, such as changing from Service Groups to Services, then you must delete the position, and create a new position. You cannot delete a position that is in use, indicated by a checkmark (✔) in the Used column.

Deleting a Functional Position

You cannot delete standardized, system-defined functional positions, which are indicated by a “grayed out” checkbox. Nor can you delete one in use, indicated by a checkmark in the Used column. You should, however, delete any functional positions that are no longer in use. To remove unnecessary functional positions simply check them and click **Remove**.

Roles

Service Portal provides “Role-Based Access Control” (RBAC). This allows administrators to control which people, organizational units, or groups can access certain modules, and what capabilities they can perform within each module. Further, those permissions can be allowed to operate on all entities (objects) of a particular type, or restricted to a set of named entities.

A role, therefore, combines access to a module with one or more capabilities, and in some cases, one or more object-level permissions.

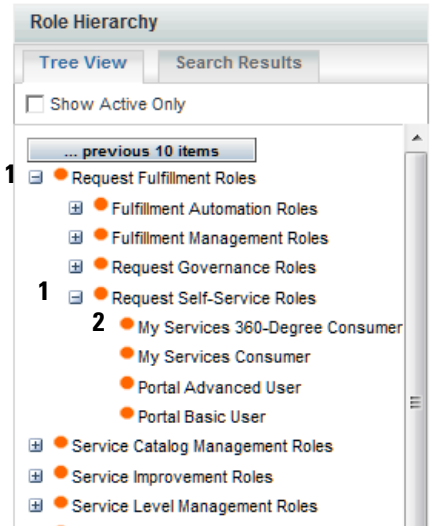
- Permissions – grants rights to act upon an object
- Capabilities – provides the means to perform certain functions within a module

Service Portal provides several system-defined roles, which group capabilities into sets of responsibilities that might typically be assigned to participants in a Service Portal implementation. Site administrators can supplement these roles with custom roles, to better suit the division of responsibilities on a particular implementation team.

Role Hierarchy

Roles are organized using a hierarchical structure of containers, much like folders. This structure allows you to create parent-child relationships between roles, in which child roles inherit the capabilities, permissions, and members from parent roles.

Containers and roles are distinguished by their name. A name ending with “Roles” is a container. The orange icon indicates a *system-defined* role.



1	Container
2	Role

System-Defined Roles

Service Portal provides system-defined roles which reflect the majority of use cases an average company may require for their users. In general, these roles should meet most companies' role requirements. System-defined roles are marked with a . Those roles which are categorized and assigned capabilities in accordance with ITIL (IT Infrastructure Library) guidelines are noted.

In the event that one of these system-defined roles does not meet your needs, you can create a new role, or, better yet, copy an existing role and modify it to meet your needs.

The following lists the hierarchical structure of the system-defined roles. Click the role name for a brief description of the role and list of associated capabilities. You can also see a list of capabilities by module.

Role Containers	Description	Roles
Demand Management Roles	Roles supporting the ITIL process of Demand Management, within the Solution Area of Service Strategy and Design.	• My Services Executive • Relationship Manager
Financial Management Roles	Roles supporting the ITIL process of Financial Management, within the Solution Area of Service Strategy and Design.	• Finance Designer • Finance Manager

Request Fulfillment Roles	Roles supporting the ITIL process of Request Fulfillment, within the Solution Area of Service Operations, including Request Self-Service, Request Governance, and the management and automation of fulfillment activities.		
	Sub-Containers	**Description**	
	Fulfillment Automation Roles	Roles supporting the automation of service request fulfillment and delivery.	• Integration Administration • Integration Specialist
	Fulfillment Management Roles	Roles supporting the fulfillment of service requests.	• Service Manager • Service Performer • Service Team Administrator • Service Team Manager
	Request Governance Roles	Roles supporting the governance of service requests.	• My Services 360-Degree Professional • My Services Professional • Portal Professional User
	Request Self-Service Roles	Roles supporting the initiation and tracking of service requests.	• My Services 360-Degree Consumer • My Services Consumer • Portal Advanced User • Portal Basic User
Service Catalog Management Roles	Roles supporting the ITIL area of Service Catalog Management, within the Solution Area of Service Strategy and Design.		• Catalog Designer and Administrator • Catalog Presentation Owner • Catalog Publisher • Distributed Catalog Manager • Distributed Service Component Designer • Distributed Service Designer • Distributed Service Request Designer • Interactive Form Specialist
Service Improvement Roles	Roles supporting the ITIL process of Service Improvement, within the Solution Area of Continual Service Improvement.		• Analyst Administrator • Service Operations Analyst • Service Strategy and Design Analyst

Service Level Management Roles	Roles supporting the ITIL process of Service Level Management, within the Solution Area of Service Strategy and Design.	• Service Level Designer • Service Level Manager
Service Lifecycle Management Roles	Roles supporting the processes of defining and managing service items in the context of the service catalog and in service delivery.	• Service Item Administrator • Service Item Designer • Service Item Manager • Service Standards Manager
Service Portal Management Roles	Roles supporting the processes of defining and managing the service portal.	• Distributed Portal Designer • Portal Content Provider • Portal Designer and Administrator
Service Portfolio Management Roles	Roles supporting the ITIL process of Service Portfolio Management, within the Solution Area of Service Strategy and Design.	• Organization Designer • Organization Manager • Portfolio Designer and Administrator • Portfolio Manager • Portfolio Presentation Owner • Portfolio and Catalog Stakeholder
Service Reporting Roles	Roles supporting the ITIL process of Service Reporting, within the Solution Area of Continual Service Improvement.	• Advanced Reporting - Business User • Advanced Reporting - Professional User • Reporting Administrator • Service Operations Report User • Service Strategy and Design Report User
		• Anyone • Site Administrator

"Anyone" and "Site Administrator" Roles

The "Anyone" and "Site Administrator" roles listed at the bottom of the chart above do not fit into an ITIL role structure. These roles provide access control capabilities unique to Service Portal.

The "Anyone" role is (quoting the description of the role): "Special Role created to support the assignment of capabilities and object-based permissions to the logical anyone, which represents all People." Every person is automatically a member of the Anyone role—you cannot modify the list of members.

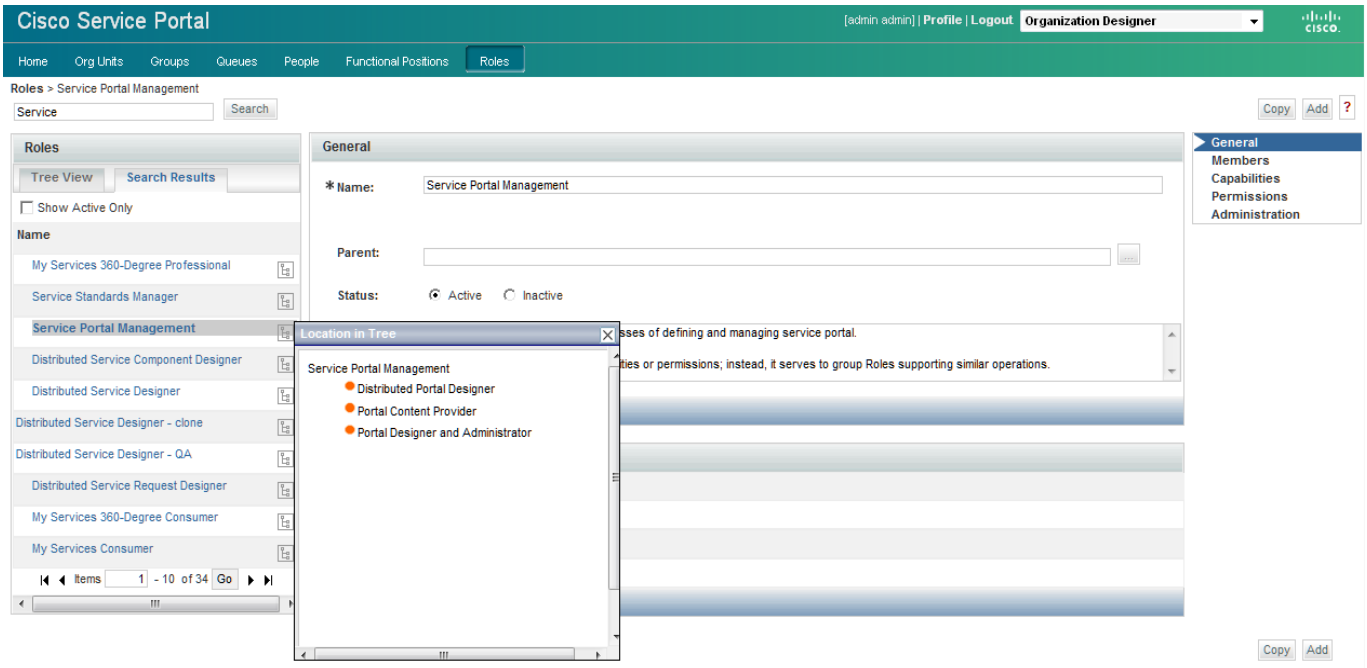
In small installations it is sometimes useful to assign to Anyone the capability to order all services. Think twice (or more) before assigning any other permissions or capabilities; any person with access to Service Portal would be able to perform the functions provided by those roles and capabilities.

The “Site Administrator” role, again quoting from the role description, is a “Role automatically assigned to any user who is a member of the Site Administration organizational unit; provides all capabilities and permissions within Request Center and Demand Center.” The “admin” user is automatically a member of the Site Administrator role. Other members should be assigned sparingly, because of the power conferred by the role.

Searching for Roles

You can search for a role by typing all or part of its name in the Search box on the Roles tab.

In the Search Results list, click the Item Hierarchy icon to view its exact location in the roles Tree View.



In the example above, “My Services Consumer” was entered into the Search field. The role was found and listed on the Search Results tab. You can see, by clicking the hierarchy icon, that this role resides in the Request Fulfillment Roles container, which resides in the Request Self-Service Roles container.

Click the role name to view general details such as the name and description, the entities that have been assigned to this role, included capabilities, object-level permissions, and to configure which entities have access to this role.

Configuring Roles

You use the Roles tab to search for and to view, create, modify, deactivate, or delete roles. Once you locate the role you wish to work with, there are five sections with which to become familiar:

General	General information about the role, including the role name and description, its place in the role hierarchy, as well as its status (Active or Inactive).
Members	People, groups, and organizational units assigned this role.

Capabilities	Capabilities included in a role. You cannot add or delete capabilities in a system-defined role, although you can sub-roles/child roles to a system-defined role.
Permissions	Object-level permissions, if any, for the role. Not every module contains objects with object-level permissions.
Administration	Entities with permission to view and/or modify role information.

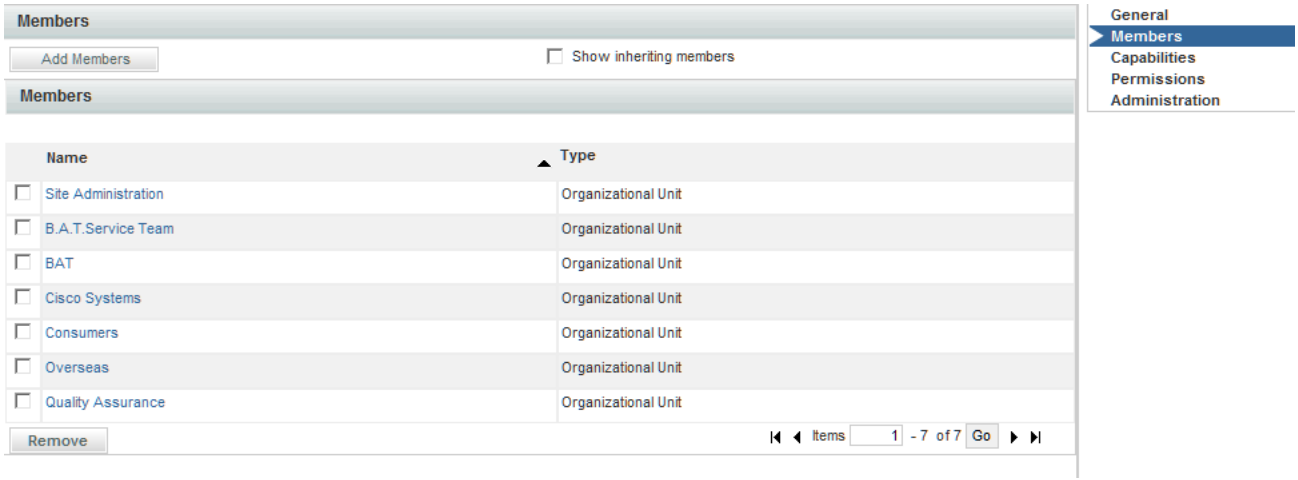
Assigning Members to a Role

Members of a role consist of individual people, groups, and organizational units that have been assigned the role. If groups or organizational units are assigned, all members of the group or unit inherit the role. In addition, sub organizational units and sub groups inherit roles from their parent. The Show inherited roles option allows you to choose whether to show those members who have inherited the role from a parent organizational unit or group. If not selected, only organizational units and groups directly assigned to the role display.

Before you can assign person, group, or organizational unit to the role, you must first make sure the entity exists.

There are two ways to create a role/member association:

- Go to the individual person, group, or organizational unit, and assign the role.
- Go to the role and add members.



The screen above is for the My Services Consumer role, which is automatically granted to every OU, and by inheritance, to every person in every OU.

About Object-Level Permissions

The following objects have object-level permissions:

Object Type	Object-Level Permission(s)
Active Form Group	View Forms Design Forms

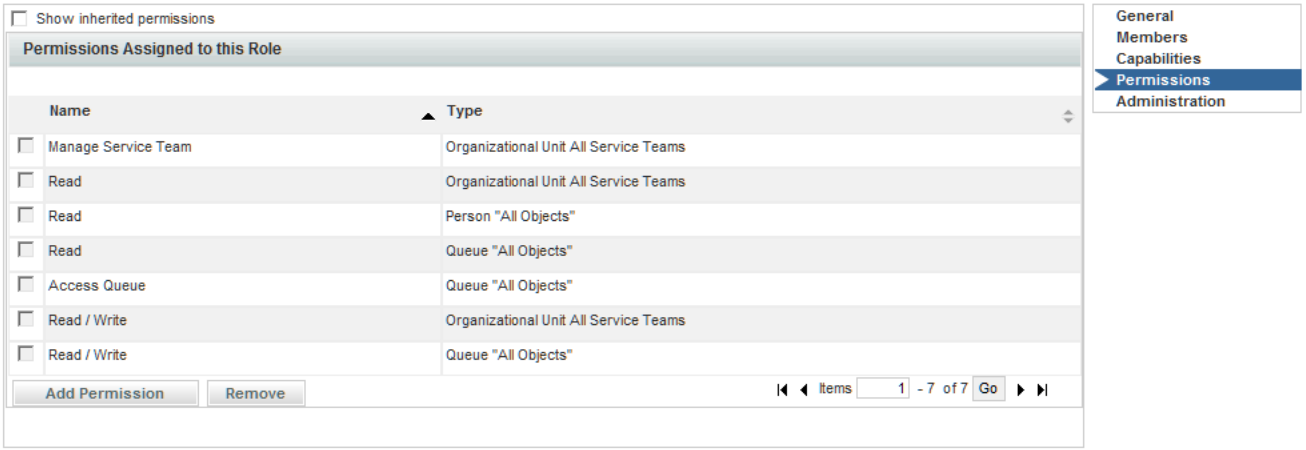
Custom Content Data	Read Read/Write
Custom Content Definition	Read Read/Write
Custom Content Group	Read Read/Write Read all definitions in this Group Read/Write all definitions in this Group
Group	Read Read/Write Change Rights
Organizational Unit	Manage Service Team Order on behalf Read Read/Write Change Rights
Person	Order on behalf Read Read/Write Change Rights
Portal Page	Read Read/Write
Portal Page Group	Read Read/Write Read all pages in this Group Read/Write all pages in this Group
Portlets	Read Read/Write
Queue	Access Queue Read Read/Write Change Rights
Role	Read Read/Write Change Rights

Service	Order Service
Service Group	Order Services View services and other information Design services and change data Assign Rights

Roles with Object-Level Permissions

Not every module contains objects with object-level permissions. Thus, not every role has object-level permissions assigned. An example of a role that does include object-level permissions is the "Service Team Administrator" role, which resides in the Request Fulfillment Roles > Fulfillment Management Roles container. The "Service Team Administrator" role includes capabilities across two modules:

If the purpose of this role is to enable the full range of management actions in Service Manager *and* the ability to create and manage service teams and queues in Organization Designer, then this role must grant object-level permissions to Organizational Units, People, and Queues, as shown below.



Capabilities

A “capability” is the ability to perform certain functions within Service Portal. It is critical to review the capabilities that are available and how they are combined in the pre-defined roles in order to be able to assign the pre-defined roles to appropriate users and potentially to recognize the need to create a custom role.

The easiest way to review the available capabilities online is to “pretend” to create a custom role, click **Add Capabilities**, and browse through the list displayed. Capabilities are divided by module, since each capability confers rights to perform functions within a particular module.

Capabilities for each module are summarized below.

Capabilities for My Services

My Services capabilities pertain to the abilities to order services; view requisitions; and access tabs and links available in the My Services module.

Capability	Description
View Requisitions	This capability controls whether the user can see the “Requisitions” link and portlet. Users with this capability can also drill down to Requisition details and track the current status.
View My Service Items	Users with this capability can see all service items they have been provisioned, in the My Service Items view (and/or Service Items portlet).
View Service Items for My Business Units	Users with this capability can see all the service items that have been provisioned or assigned, to OUs or members of OUs of which they are member.
See Requisitions for My Business Units	Users with this capability can see all requisitions for their business units in the My Requisitions view.
View and Perform Authorizations	This capability controls whether users can see the “Authorizations” link in the top navigation bar.
See Authorizations for My Business Units	Users with this capability can see all authorizations for their business unit in the Authorizations view.
Order on Behalf of Others	Users will see the Order on Behalf link in the top level navigation bar. Simply having any Order On Behalf object permission will also cause the Order on Behalf link to appear.
Order My Services for Others	Users can order any service they have ordering permissions for on behalf of other users, in addition to the services that those other users can order for themselves.
View KPIs	The KPI portlet appears in the My Services, My Services Executive, Relationship Manager, and Service Level Manager home pages. (This capability is effective only if the **Show KPI Portlet** global setting is turned **On**.)
Browse for Services	This capability controls if the user can see the Browse Services portlet.
Search for Services	This capability controls the Search Services portlet.
Order Services	This capability controls whether the user receives the “Order” link next to services that are orderable.

Copy Requisitions	This capability controls if the user sees the “Copy Requisition” link in the top navigation bar and all associated functionality for Copy Requisitions.
Manage Profile	This capability controls whether users can manage their profile which is available via the “Profile” link.

Capabilities for Service Designer

The Service Designer capabilities allow different sets of users to work on different aspects of a service definition. Coupled with the ability to assign permissions to different sets of users to work on different sets of services and service groups, this provides robust support for a distributed development environment.

Capability	Description
Access Services	This capability grants access to the Service Catalog option within Service Designer. Any user with this capability has access to all of the services in any of the service groups to which he has the “Design services…” or “View services…” permission. This capability provides access to all tabs within the service definition.
Access Service Presentation	This capability grants access only to the General, Offer, and Presentation tabs for a service. A user with this capability has access to those tabs on all services in any of the service groups to which he has the “Design services …” or “View services…” permission.
Access Service Forms	This capability grants access only to the Service Form tab for a service. A user with this capability has access to that tab on all services in any of the service groups to which he has the “Design services…” or “View services…” permission.
Access Service Delivery	This capability grants access only to the Plan and Authorization tabs for a service. A user with this capability has access to those tabs on all services in any of the service groups to which he has the “Design services…” or “View services…” permission.
Service Administration	This capability grants access only to the Permission tab for a service. A user with this capability has access to that tab on all services in any of the service groups to which he has the “Design services…” or “View services…” permission.
Access Service Groups	Grants access to service groups. A user with this capability has access to all service groups to which he has the Read or Read/Write permission.
Access Active Form Components	Grants access to Active Form Components. A user with this capability has access to all form groups to which he has the Read or Read/Write permission.
Manage Service Dictionaries	Grants Read/Write access to all dictionaries, at all system moments. Supports the ability to test and debug services.
View Dictionaries	Grants read-only access to dictionaries.
Manage Dictionaries	Grants permissions to edit and create dictionaries.
Manage Scripts	Grant permissions to all functionality of Scripts, including functions and libraries.

Manage Categories	Grant permissions to all functionality of Categories.
Manage Keywords	Grant permissions to all functionality of Keywords.
Manage Objectives	Grant permissions to all functionality of Objectives.
Import Services	Enables the Import feature of Service Designer, allowing the user to import an XML formatted service definition.

Capabilities for Service Link

The Service Link capabilities allow different sets of users to be designated as integration developers as opposed to Administrators, responsible for monitoring the status of integrations in a production environment.

Capability	Description
Monitor Integration Activities	This capability grants access to the Home and External Tasks pages and all the associated functionality in these screens.
Manage Adapters	This capability grants access to the Adapters tab and permissions to view, edit, create and delete Adapters.
Manage Agents	This capability grants access to the Agents tab and permissions to view, edit, create and delete Agents.
Manage Transformations	This capability grants access to the Transformation tab and permissions to view, edit, create and delete Transformations.

Capabilities for Reporting

Reporting capabilities allow grantees to access the Reporting and Advanced Reporting modules and to develop reports.

Capability	Description
Reports Designer	This capability grants access to all functionality available in the Report Designer section in Advanced Reporting.
KPI Administration	This capability grants all access to the KPI Administration function as well as the capability to manage the KPIs and create/modify KPIs.
View Demand Center Cubes	This capability grants access to the Analytical Cubes section of the Analytics module and provides ability to view and execute Demand Center cubes.
Ad-hoc Reports	This capability grants access to the functionality available in the Ad-hoc Reports section in Advanced Reporting.
Reporting - Administration	This capability grants access to all reporting capabilities—manage Reporting folders, dashboard, IBM Cognos Administration, schedule reports, save reports, permissions administration, and create reports.

View Request Center Reports	This capability grants access to the Reporting module and the ability to view the KPI dashboard and run Request Center reports.
View Demand Center Reports	This capability grants access to the Reporting module and the ability to view the KPI dashboard and run Demand Center reports.

Capabilities for Service Manager

The Service Manager module allows task performers to view and update internal tasks assigned to them. Task Managers can view or update tasks, as well as managing task allocation and scheduling.

Capability	Description
Search All Performers	Users can query any Performer in the system from the search box in the Navigation Pane.
Perform Work	Users have access to the following system behaviors: 1. Check In/Out Tasks 2. Close Out Tasks 3. Standard Views 4. Cancel Tasks for which they are the Task Supervisor
Manage Work	Users have access to the following system behaviors: 1. Assign Work 2. Set Task Priorities 3. Reschedule Task Due Dates 4. Administration View 5. Service Teams View
Access All Requisitions	Users can see all requisitions. In Service Manager, this capability enables a "Global Search Option" that allows searching through all requisitions and tasks in the system, regardless of the user's Queue access rights. The capability also enables the user to save public Service Manager views.
Create Ad-Hoc Tasks	Users have access to the Ad-Hoc Task creation feature in Service Manager. Once granted this capability, the "New Ad-Hoc Task" form section on the Ad-Hoc Task page is available to the user.

Capabilities for Organization Designer

Organization Designer capabilities allow access to the options for maintaining people, organizations, queues, roles, and functional positions. These options supplement the ability to maintain these objects provided through Directory Integration (described in the *Cisco Service Portal Integration Guide* and performing Directory Tasks (described in the *Cisco Service Portal Designer Guide*). Together with object-level permissions, allowing users to read and/or write specific organizational entities, the capabilities provide granular control over a multi-tenant environment.

Capability	Description
Manage Basic Service Deployments	Allows the ability to create, transmit and manage Basic Service deployment packages.
Access Organizational Unit Configuration	Users see the Organizational Units tab and entity type in a homepage search within Organization Designer and can access the OU's they have rights to.

Access Groups Configuration	Users see the Groups tab and entity type in a homepage search within Organization Designer and can access the Groups they have rights to.
Access Role Configuration	Users see the Roles tab and entity type in a homepage search within Organization Designer and can access the Roles they have rights to.
Access Person Configuration	Users see the People tab and entity type in a homepage search within Organization Designer and can access the Persons they have rights to.
Access Queues Configuration	Users see the Queues tab and entity type in a homepage search within Organization Designer and can access the Queues they have rights to.
Access Functional Position Configuration	Users see the Functional Position tab within Organization Designer.

Capabilities for Administration

Individual capabilities are not available for all options within the Administration module. For options not covered by a capability (for example, access to the Debugging page), users must be granted the Site Administrator role.

Capability	Description
Manage Directory Integration Configuration	Users see the Directories option and can configure Directory Integration settings.
Manage Authorization Structure	Users see the Authorizations option and can configure site level Authorizations.
Manage Global Settings	Users see the Global Settings option and can configure site level application settings that alter system behavior.
Manage Email Templates	Users see the Email Templates option and can view, create, or disable email templates.
Manage Lists	Users see the Lists option and can view and modify system reference lists.
Use Support Utilities	Users see the Utilities tab and Use Support Utilities link.
Access Log and Property Files	Users see the Log and Property tab and view and download log and property files.

Capabilities for Catalog Deployer

Catalog Deployer capabilities allow grantees to build and/or deploy packages within the Catalog Deployer module.

Capability	Description
Manage Basic Service Deployments	Allows the ability to create, transmit and manage Basic Service deployment packages.
Manage Advanced Service Deployments	Allows the ability to create, transmit and manage Advanced Service deployment packages.
Manage Custom Deployments	Allows the ability to create, transmit and manage Custom deployment packages.

Import Deployments	Allows for the import and export of deployment packages.
Deploy Deployment Packages	Allows the deployment of a new or updated content into the site.
Manage Basic Offering Deployments	Allows the ability to create transmit and manage Basic Offering deployment packages.
Manage Advanced Offering Deployments	Allows the ability to create transmit and manage Advanced Offering deployment packages.

Capabilities for Portal Manager and Portal Designer

Capabilities for the use of Portal Designer and the Portal Manager are described in detail in Portal Manager.

Custom Roles

Organization Designer provides a large number of predefined roles. These roles should be suitable for most use cases an average company may encounter for their users. If, however, you need additional roles, you can create custom roles by either creating a new role from scratch or copying an existing role and modifying it to meet your needs.

Because of the numerous combinations of capabilities and permissions available, keeping track of these combinations can be a challenge. Therefore, you should create a new role by identifying a system-defined role that has most or all of the capabilities you need. You should not use a system-defined role with more capabilities than you need is because you cannot remove capabilities from a child; it inherits all of the capabilities of its parent.

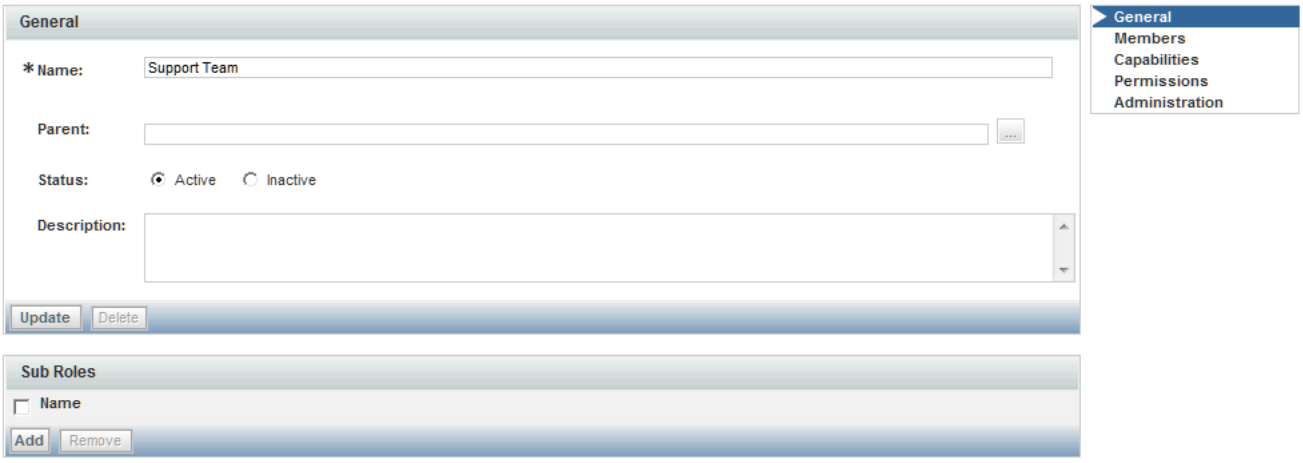
1. Create this role by doing one of the following:
   - Create a new role from scratch
   - Copy a similar role to use as a template for a new role.
2. Make the user-defined role a child of a system-defined role.
3. Define the new role by adding capabilities and permissions as needed.
4. Assign members to the role.

General Role Information

Enter the following information:

Name	Name of the new role.
Parent	Click the ellipses to search for and select the system-defined parent role that most closely resembles the new role you wish to create.
Description	Any text describing the new role.

For custom roles, the General page allows you to edit information provided when the role was created. You can assign a parent role, set the role to be active or inactive, or add to the roles description, logging any changes as they occur. You can also develop the hierarchical structure by adding or removing sub roles.



Role Hierarchies

Sub roles allow you to create a hierarchical structure of parent and child roles. Each role can have both a parent role and one or more child, or sub, roles. Only custom roles can be used when creating a sub role hierarchy. The hierarchical structure of system-defined roles cannot be changed.

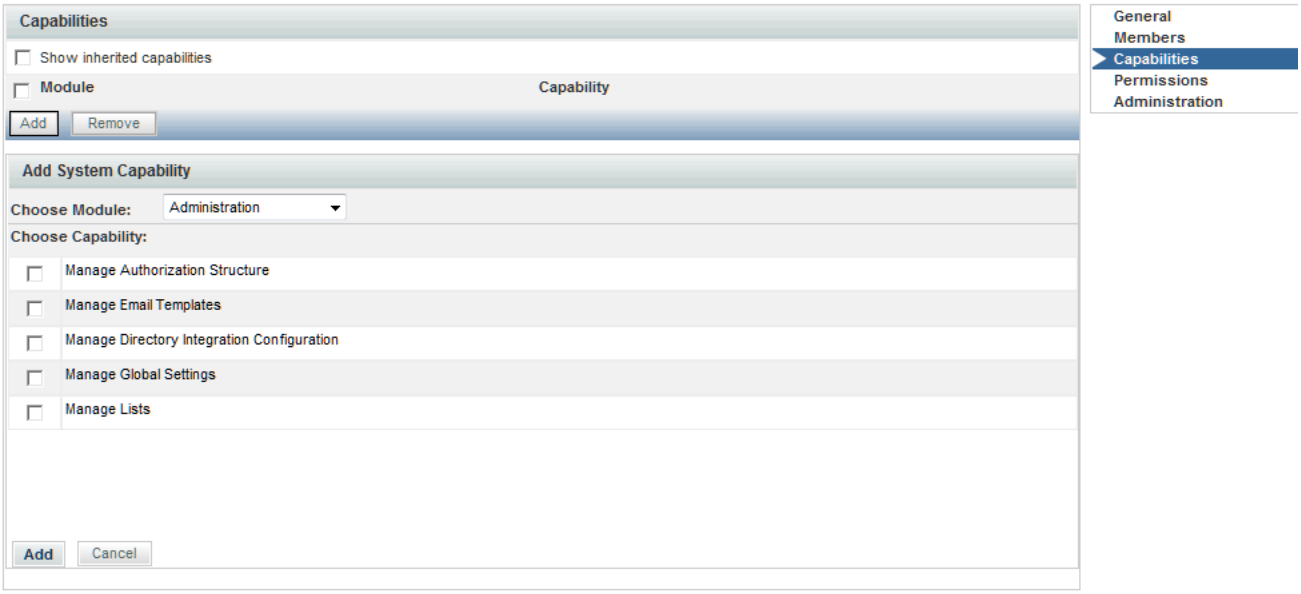
Sub roles, and therefore the members of that sub role, inherit all the capabilities assigned to its parent role. Because of this inheritance rule, you must make sure you set up your role system carefully.

You can create a parent/child relationship using two methods:

- Assign a parent role on the General page.
- Assign child, or sub, roles to the parent.

Assigning Role Capabilities

Capabilities define the activities that can be performed within a specific module. Capabilities for system-defined roles are pre-defined, and cannot be changed. For custom roles, you can specify the desired capabilities:



Assigning Permissions

Permissions grant the rights to an object, such as an organizational unit or group, within a particular module. These include read/write access to other modules, as well as object-specific permissions. These include:

Module	Object Type	Permission Available for Assignment
Organization Designer	Organizational Unit	Who can order on behalf of the organizational unit Who is responsible for managing a particular service team
	People	Who can order on behalf of a person Who is the Authorization Delegate for a person
	Queue	Who can access a particular queue within Service Manager
Service Designer	Service	Who can order a particular service
	Service Group	Who can order a particular service Who can view services and other information in this service group Who can design services and change data in this group Who can assign rights
	Active Form Group	Who can view forms in the group Who can design forms in this group

To add a new object-level permission to a custom role, use the table above to select the following:

Object Type	Select an object (entity) type from the list box.

Permission for this type	Based on the object type selected, select the permission.
Assign permission to	Choose one of the following: All objects of this type – For example, if you choose organizational unit, then all organizational units are assigned this permission. Selected Objects – Search for and select the objects to which you wish to assign this permission.

Modifying an Existing Role

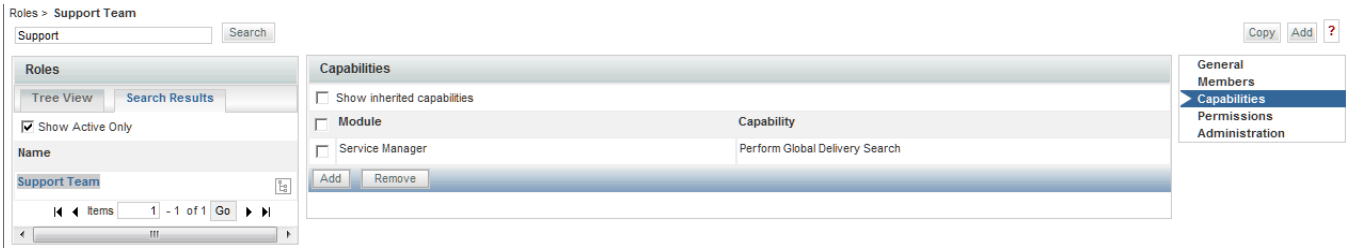
For system-defined roles, you can only modify the members assigned to the role, as well as read/write access to the role. Custom roles are fully modifiable, including capabilities and permissions, for those users with the correct administrative rights to do so.

Sample Custom Roles

Support Team

We have a support team that handles issues faced by clients. That team must be able to view every requisition but not modify the requisition in any way. This role needs read access to all requisitions.

1. Create a new role with one capability: *Perform Global Delivery Search*. This will allow any member of this role to access the Service Manager module and search for all tasks/requisitions.



2. Assign your support team as members of this role.

Organization-Specific Service Team Administrator

The “Service Team Administrator” pre-configured role, described in the section above on Object-Level permissions, allows members of the role to manage any service team and to modify information on any organizational units and queues.

This role is an excellent candidate to be copied to a custom role which provides the same capabilities but limits its members to working on specific organizational units, and queues, rather than “All Objects” of each type. Responsibility for maintaining the service teams in an organization could be divided between multiple Service Team Administrator roles, each of whom has control over a different set of organizations and their queues. If the organizations were structured hierarchically, only a parent organization would need to be specified as the object of a particular permission—all child objects would also be subject to the same permission.

Support Team for an External Application

Assume that many, but not all, requisitions have an integration to an external system such as Remedy. Analysts who work on the Remedy application may need to review any Request Center requisition that includes an integration to Remedy, and may need, for example, to add attachments or comments to such requisitions.

1. Create an OU of type = Service Team, named, for example, **Remedy Team**.
2. Make all the people who need access to these requisitions members of this OU.
3. Create a queue homed to the Remedy Team OU; name it **Remedy Team**. The Remedy Team OU now automatically gets the Access Queue permission to the queue of the corresponding name.
4. For any service for which the Remedy integration is part of the delivery plan, add a task.
   a. Assign the performer to be the Remedy Team queue.
   b. Make the task conditional upon 1=0.

Here's why this works: Request Center grants access to a requisition based upon whether the user has "an affiliation" with the requisition—that is, if he is the customer, or the initiator, or **if he plays a role in the delivery of the requisition**. If a person is a performer (or has access to a queue that is a performer) of a task in the requisition, that person therefore has access to the requisition.

An alternative approach with equivalent results is to substitute the following step for Step 4 above:

- For any service for which this issue will arise, assign the plan-monitoring task to the Remedy Team queue.

Distributed Service Design

In an implementation of Request Center that spans multiple divisions within an organization, it is sometimes desirable to distribute the responsibilities for service design to multiple groups of developers. Ideally, these developers should be able to leverage each others' work—reusing a service or service component created and tested by another group —while being prevented from accidentally or on purpose changing a design component maintained by another group.

Such an environment can be established via the use of Permissions associated with Service Designer components. You could set up a custom role for each development group. (Members may be assigned either directly or indirectly, via membership in a service team or group.) In Service Designer that role is able to:

- Design services … in this service group (service groups containing services maintained by the team)
- Order services in this service group
- View services in possibly related services groups, or groups that might have interesting techniques for them to see
- Design forms in their own form group(s)
- View forms in the reserved group
- View forms in any other (common?) groups that they might need to include in their services

Rather than giving the custom role a pre-existing Service Designer role, it would be preferable to grant appropriate Service Designer capabilities to the role. This option may be more work to set up, but gives you more flexibility. One thing to be careful about is in granting the group the right to import services. You could import a service and overwrite components (dictionaries or forms) that you do not normally have the ability to modify—the Import Service option does not check object-level permissions, it just overwrites (or creates) everything.

Support for Web Services

In addition to users being able to submit requisitions via My Services, Service Portal provides the ability for external systems to submit requisitions via a web service request, using the Requisition API (RAPI). Such requests, bypassing My Services, would never have a service form displayed in the ordering moment. Consequently, their design would need to differ from that of a corresponding service that is ordered interactively—for example, no rules or JavaScript functions could provide default values; and multi-option fields, such as check boxes or drop-down lists, could not be used.

As a result of those limitations, designers sometimes choose to create a set of parallel services that can only be ordered via RAPI. Such services should never appear in the Service Catalog of non-administrative users. Instead, ordering permissions should be granted only to administrative users. The RAPI service is always ordered by such a user who has been assigned the critical capability to "Order my services for others", with the "other" specified as the customer for the request.

Authorizations

Authorizations are tasks that require the assigned authorizer to reject or approve a service request. Reviews are tasks that require the performer to indicate that they have reviewed a step in the delivery process.

Request Center supports several types of authorizations and reviews.

Financial Authorization	Authorization to determine if a requested service or item is within budget. This authorization cannot be overridden at the organizational unit level.
Departmental Authorization	Authorization by business unit manager for purchase approval.
Departmental Review	Review of requested service or item by a department to see if it is appropriate.
Service Group Authorization	Authorization by a service team manager for purchase approval. Usually, the service team manager authorizes for people who are on his service team.
Service Group Review	Review of requested service or item by a service group to see if it is appropriate.

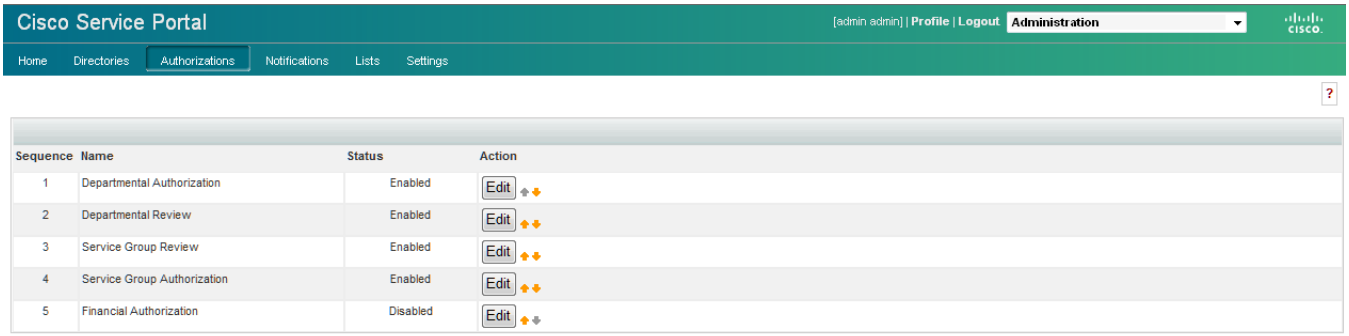
Setting Up an Authorization Structure

Setting up an authorization process consists of three steps.

1. Start by using the Administration module to specify which types of authorizations will be available, and the order in which they should be performed.
2. Then, specify the details for each type of authorization which has been enabled.
3. Optionally specify the escalation procedure to be followed if a required authorization is late.

Enabling Authorizations

Up to five authorization types can be enabled for a site. To change the order of execution, click the Up or Down arrow to the right of the Authorization/Review until it is in the correct sequence.



Specifying Authorization Details

If an authorization/review type is enabled, you can then specify details for that authorization/review type. Authorization details can be defined:

- At the site-level (using the Administration > Authorizations option)
- For each organization (for Departmental Authorizations/Reviews)
- For a service group or service (for Service Group Authorizations/Reviews)

For Departmental or Service Group Authorizations you have the option to:

- Use only the site-wide authorization structure created in Administration
- Use only the authorization structure established for the organizational unit/service group
- Use the site-wide authorization structure, but supplement it with organizational unit/service group specific authorizations.

If you choose the Use site authorization structure only option, then no further steps are required. Otherwise, you may select the Authorization Type you wish to configure:

- An authorization – Authorizations are processed sequentially within the approval moment. Each authorizer must either Reject or Approve the request. If the request is approved, it passes to the next authorization or next step in the delivery process. If the request is cancelled, no further tasks are performed.
- A review – The review process runs concurrently within the approval moment. Reviewers simply click OK to signify that they have reviewed the request—they do not have the capability of stopping the delivery.

Note All authorization and review tasks must be completed before the delivery process begins.

Supply the detailed definition for the designated authorization type:

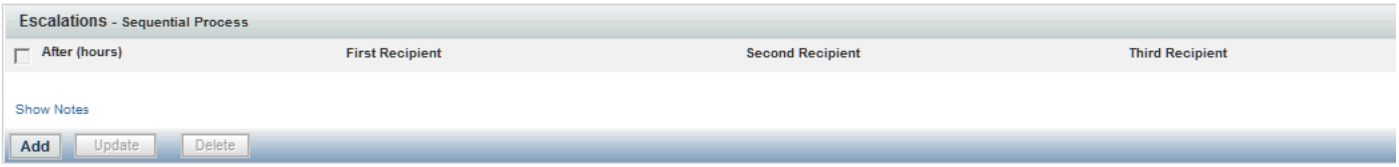
Name	Name for the new responsibility being performed by the authorizer or reviewer.
Duration	Amount of time, in hours, allotted for the authorization or review task.

Subject	Name of the authorization or review task that this responsibility performs. This value appears in the Task List that authorizers and reviewers see in Service Manager. You can use namespace variables in the task titles. A string enclosed in hash marks (#) denotes a namespace variable. The variable is replaced by the service name being ordered. See the *Cisco Service Portal Designer Guide* for details.
Effort	Amount of time that it takes to perform the review or authorization. This is typically less than the Duration.
Workflow Type	Select internal if the authorizer is someone within the system, or choose an available external workflow to perform the authorization via a Service Link task.
Assign	Select one of the following: • A person/queue – authorization or review will be fulfilled by the designated person or queue. • From a position – authorization or review will be fulfilled by the designated functional position. • From an expression – authorization or review will be fulfilled based on the value of the expression entered.
Assign to	Click to select the value that corresponds to your selection for the Assign field. If you select **From an expression**, type the expression. Expression syntax is documented in the *Cisco Service Portal Designer Guide*.
Escalation Tiers	Click one of the following: • Use all – All escalations set up for this process are used. • Use only – If you do not wish to use all the escalation tiers set up for this authorization or review process, enter the number of tiers you do wish to use.
Condition	Expressions containing conditions which need to be met for approval. Using True or False, it indicates if the task will occur or not. If you do not enter an expression, the default value is True and the authorization will always be executed. Click **Validate** to verify that the expression you are using will work. Validation only executes a syntactical check; the validation function does not check to see if the data you are referencing actually exists in the request.
Evaluate condition when	Choose either: • Authorization phase starts (if condition evaluates to “false”, times will be computed as zero). The condition entered in the Condition field becomes active as soon as the authorization phase begins. • Activity becomes active (times will not be affected, scheduling will be done by using these efforts) – The condition entered in the Condition field becomes active when the authorization phase completes and the activity after the authorization begins.

Re-evaluate expression as authorizations/ reviews proceed	Select the checkbox if you wish the performer name or task name to be re-evaluated after every authorization task, and updated as necessary. Due dates for the authorization do not change. This setting should be used if the performer is assigned via an expression, and a previous authorization step may have allowed the authorizer to change the value of a field used in that expression.
Notify when authorization starts	Email templates that are automatically sent when the mentioned task is complete. A list of email templates available in the system displays in the box.
Notify when authorization completes	
Notify when requisition is rejected	
Notify when task is rescheduled	
Notify when task is reassigned	
Notify when external tasks fail	

Escalations

Escalations are a process whereby a certain activity that has not been performed within the designated duration is flagged and sent to the appropriate performer, supervisor, and/or customer for resolution. Recipients receive notification of the delayed task in the form of an email.



When setting up an escalation process, keep in mind the following:

- Each row in the escalation list represents a tier. You can have as many tiers as you want—simply click **Add** to add another tier. (You may delete a tier by checking the corresponding check box and clicking **Delete**.)
- The first tier represents the first group to be notified when a task exceeds its standard duration. The time—**After (hours)**—represents the number of hours after the due date before the notification is sent.
- After the first notification, the time specified for subsequent tiers represent the time elapsed since the previous escalation. For example, if the second tier has 8 hours as the time, then 8 hours after the first notification is sent without a resolution triggers the second group notification.
- Up to three recipients can receive an escalation notification for each tier. For each Recipient box, you enter a list of valid email addresses, separated by commas. Namespace references of the type #variable# are also permitted. For example, #Perfomer.Manager.Email# would direct the notification to the manager of the task performer.

- For each recipient, use the corresponding drop-down box to select the Emails used to notify the recipients. The notifications are derived using templates created within the Administration module.

Escalations are actually sent out by the Escalation Manager, which is part of the Business Engine, the workflow manager. By default, the Escalation Manager checks for late tasks with associated escalations once an hour, on the hour, during normal work hours. So, it is not quite correct to state, as above, that an email notification will be sent after the authorization has been late for the designated number of hours. The notification will actually be sent the next time the Escalation Manager checks for late tasks after the escalation period has expired. For example, if an authorization was due at 12:30 PM, and an escalation notice is set to be sent 1 hour later (at 1:30 PM), the notification will actually be sent at 2 PM, the next time the Escalation Manager runs.

The administrator can change Escalation Manager settings. The procedure for doing so is documented in Chapter 5, “System Administration”.

CHAPTER 2

User Profiles

- Overview, page 2-1
- Information, page 2-1
- Preferred Language, page 2-2
- Calendar, page 2-3
- Preferences, page 2-3

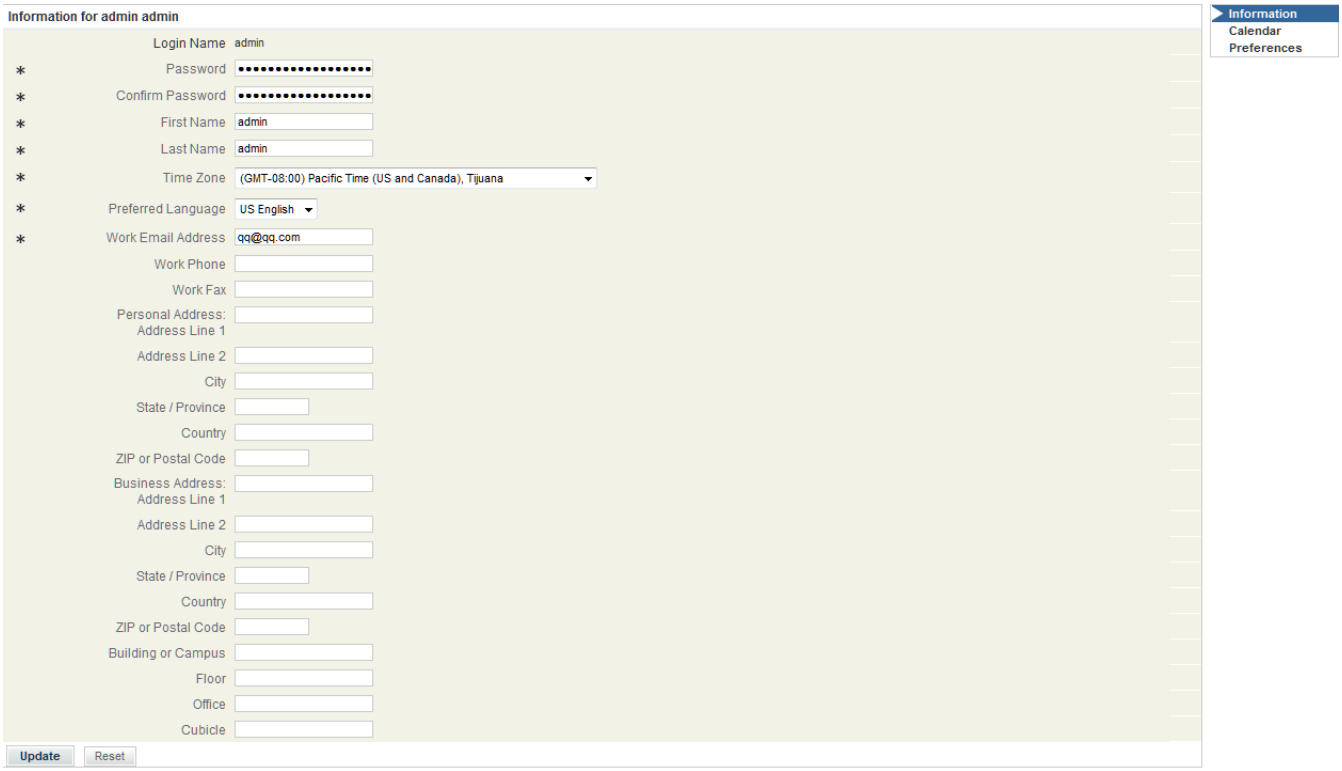
Overview

The “Profile” link on the top banner allows all users to access and change their profile.

A user Profile contains personnel Information, Preferences, and the work Calendar. You can change your user Profile at any time. The site administrator can also modify any Profile information using the People component of Organization Designer.

Information

In a system where directory integration is configured to import person information, users should not change their personnel program using the Information page. Any such changes would be lost the next time the user profile was refreshed. Instead, contact your site administrator for assistance in updating your Profile information.



You must provide information for every field marked as required (*). In particular:

- You will need the User Name and Password to log on.
- The Work Email Address is used to send automated email notifications about your service requests.
- The Home Organizational Unit is usually the same as your department's name. This information is used by the system when services you request must be reviewed or approved by your supervisor or manager.
- The time zone is used to display scheduled start and due dates. For service performers, it is also used to determine the performer's work hours and compute the work time spent on a particular task.

Preferred Language

The My Services module is available in multiple languages. By default, only US English is available in the Preferred Language drop-down list. Other languages can be made available by adding them to the Language List in the Administration module. See the "Language" section on page 3-7.

For My Services, the supported languages are as follows:

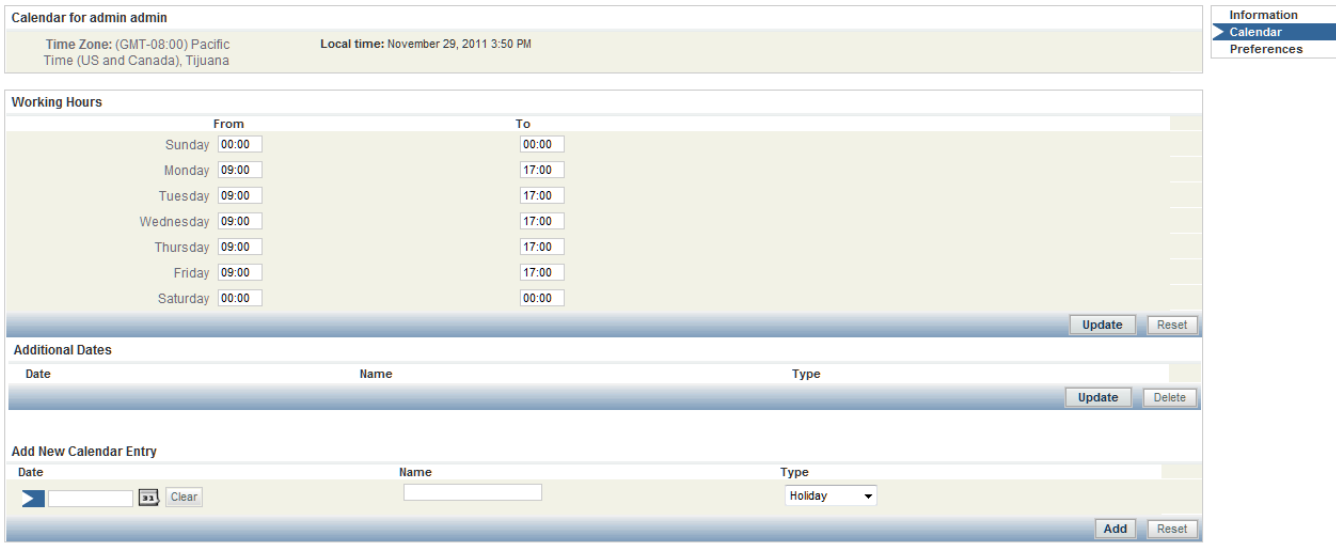
- US English
- German
- French
- Spanish
- Dutch
- Chinese (Simplified)

- Chinese (Traditional)
- Brazilian-Portuguese
- Japanese
- Korean

For all other modules, the only language supported is US English.

Calendar

Calendar settings establish the availability of service team members to perform work.



You can:

- Set your work hours and work days.
- Set the holidays on which you are not available.

When entering Calendar information, the following applies:

- Under Working Hours, change your standard working hours and days by entering new times in military time format in the From and To fields. For example, you would enter 23:00 for 11:00 p.m. To indicate a 24-hour day, type 12:00 as the starting time and 23:59 at the ending time.
- Type 0:00 in the From and To fields for days that you do not work.
- Under Add New Calendar Entry, you can change a Working Day to a Holiday, and vice versa.

Preferences

Preferences govern the behavior and appearance of Service Portal.

Preferences can control:

- Date Formats.
- Your Login Module – Users can select any module which they can access to be displayed automatically as soon as they log in.
- Your Default Service Manager View – Service performers can set the system to automatically go to the Service Manager view they use most frequently.
- Your Default Service Manager Status (for task search) – Service performers can set the task status search condition they use most frequently.
- Time Format – 12- and 24-hour clocks are available.
- View Portlets – Allows you to suppress the appearance of the Authorizations and Service Items portlets on the My Services home page. The Authorizations and Service Items lists are still available via the corresponding tabs if the user has been granted access to these capabilities.
- Authorization Delegate information – This person can perform authorizations for you during the time period you specify using the Delegation Start Date and Delegation End Date fields.

CHAPTER 3

Site Administration

- Overview, page 3-1
- Directory Integration, page 3-2
- Site-Wide Authorizations, page 3-2
- Email Templates, page 3-2
- Lists, page 3-5
- Site Settings, page 3-8
- Support Utilities, page 3-23

Overview

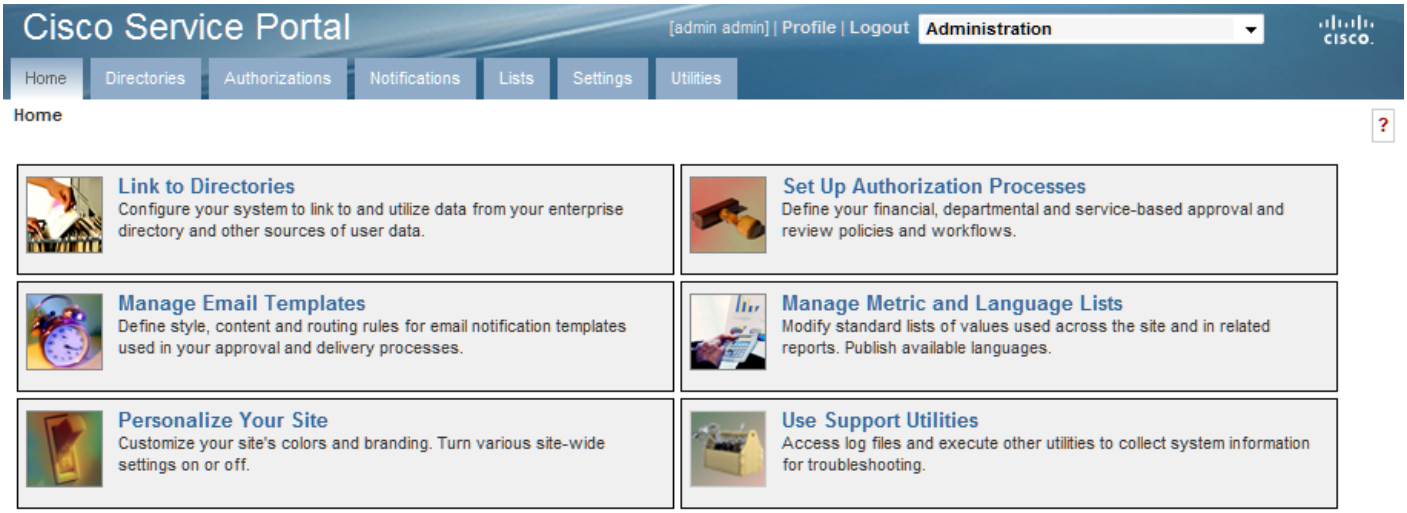
The Administration module allows you to set up a variety of behaviors to accommodate the rules and business practices of your company.

Using the Administration module, you can:

- Link to and utilize data from your enterprise directory and other sources of user data.
- Define approval and review policies and workflow.
- Define email notification templates used in your approval and delivery processes.
- Modify standard lists of values, and publish available languages.
- Customize site-wide settings, including establishing custom stylesheets to be used by specific organizational units or groups of those units.
- View and copy system log and property files for troubleshooting.

Administration Home

The Administration Home page allows you to navigate throughout the module, using either the tabs on the navigation bar or the links within the Content Pane.



Directory Integration

Directories are repositories of user data. Administration allows you to configure your system to link to and utilize data from an enterprise directory and other sources of user data. In particular, you can synchronize user profile information with the directory server database.

For detailed information about Directory Integration, including worksheets to help you organize the information necessary for integration, detailed mapping information, and special considerations, see the *Cisco Service Portal Integration Guide*.

Site-Wide Authorizations

The Authorizations option of the Administration module enables or disables authorizations and reviews, and allows administrators to set up site-wide authorizations. Such site-wide authorizations can be used in addition to or instead of authorizations established for individual organizations and services or service groups.

For more information please see the "Setting Up an Authorization Structure" section on page 1-48.

Email Templates

Service Portal includes a set of preconfigured email templates. You can set up a service's delivery plan to automatically send these in response to events that occur. The Administration module allows you to create new and modify provided templates used in email notifications. These emails are used to inform recipients of steps within the approval and delivery process.

Templates used by Request Center are found under the General link. Templates used by Demand Center are found under Agreement Email Templates. You can set up Administration so that the system automatically sends these in response to events that occur. For example, when a service requires

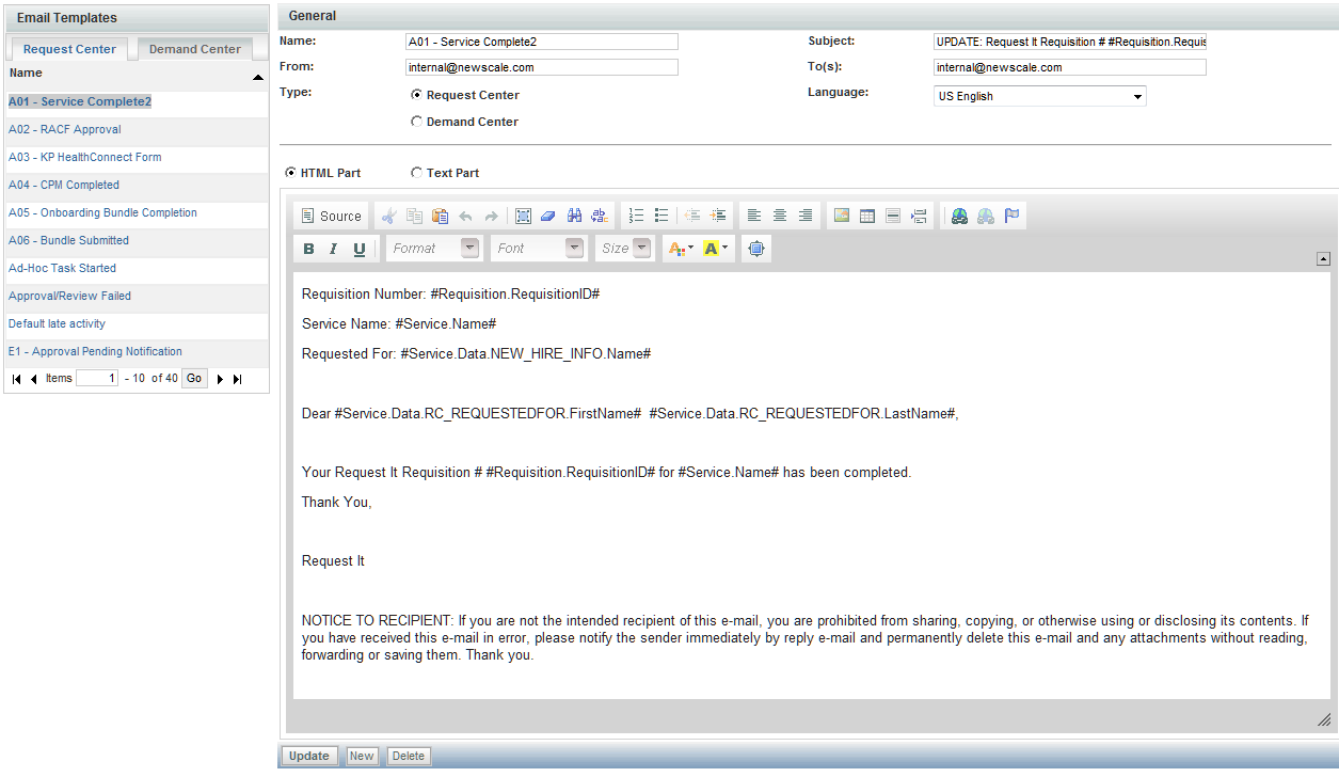
authorization from a manager, the system can send the manager an email notifying that a service request requires approval. You can change the included templates or add templates suitable for your organization.

Viewing Email Templates

You can view email template information using one of the following methods:

- On the Home page, click **Manage Email Templates**. On the Email Templates navigation pane, click the *template name* you wish to open to view.
- On the navigation bar, click **Notifications**. On the Email Templates navigation pane, click the *template name* you wish to open to view.

Clicking the *template name* displays the template styling options and content. A sample Request Center template is shown below.



Configuring Templates

To configure an email template, supply the following information:

Name	Name of the new email template.
Subject	Email Subject; may use namespaces.
From	Sender's valid email address.

To	Recipient(s)'s valid email address; multiple recipients can be separated by semi-colons; typically uses namespaces.
Type	Request Center or Demand Center.
Language	Display language.
HTML Part	Click to show the template as it would appear in an HTML-aware email system. When selected, HTML Editor tools display to allow you to format the email template.
Text Part	Click to show the HTML tags and text used to format the template.

You can delete any email template that you created and that is not in use. Pre-configured templates cannot be deleted.

Service Portal sends the email notification formatted as a MIME multi part message with both a text part and an HTML part. Most email clients ignore the text part and display the html part.

For instructions on using the HTML editor, please see the *Cisco Service Portal Designer Guide*.

Using Namespaces

See the *Cisco Service Portal Designer Guide* for details on formatting emails with dynamic data content.

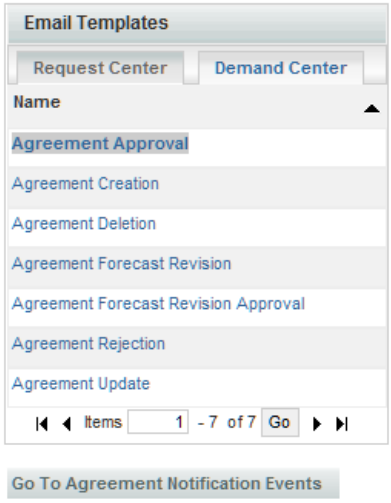
The recipient(s) of the notification will (obviously) depend on the event which triggers sending the email. For example, the customer (#Requisition.Customer.Email#) should typically receive notifications about significant changes in the status of a request.

If the event is an authorization or review, it may be prudent to include the authorizer's delegate in the list of recipients (#Requisition.Alternate.Email#). If no delegate is currently designated, the namespace value will be blank and will not affect the appearance of the notification.

Demand Center Templates

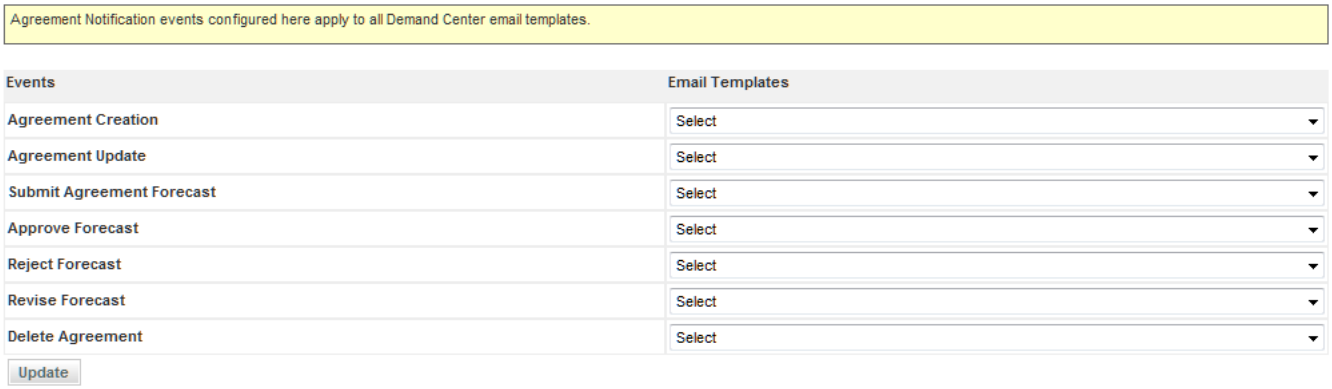
The model for using email notifications is more robust for Request Center than for Demand Center. For Request Center each individual service may be configured with a different set of notifications. For Demand Center this configuration is site-wide: the same set of notifications is used for all events, regardless of the agreement to which they pertain. To associate email templates with events:

Step 1 Click the **Demand Center** subtab to display the Demand Center templates.



Step 2 Click the **Go to Agreement Notification Events** button at the bottom of the list of templates.

Step 3 The list of agreement notification events is displayed, as shown below. You can designate an email template to be attached to each event.



Lists

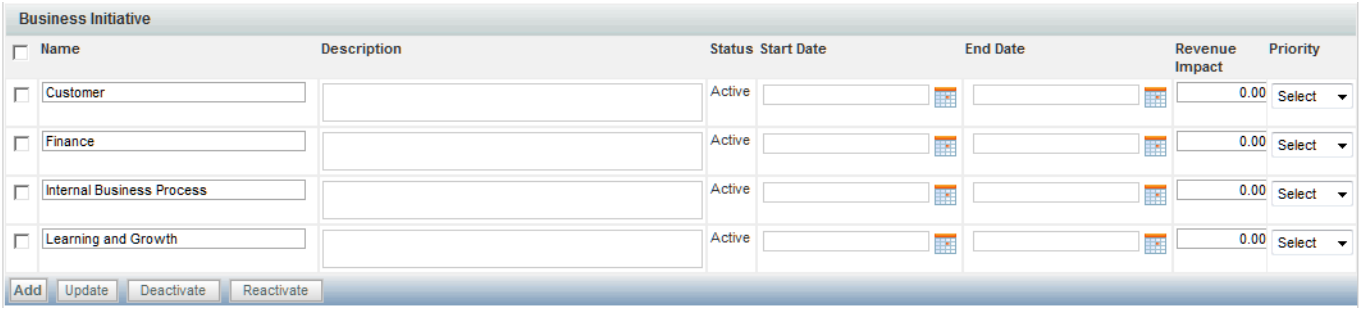
Administration allows you to modify standard lists of values used across the site and in related reports and publish available languages.

Use the Lists tab to configure the following lists:

List name	Description
Cost Drivers	Cost Drivers are available when configuring Cost Details for services in Service Designer, and when configuring Price for Service Offerings in Portfolio Designer. Cost Drivers in Service Offerings are the most relevant and meaningful attributes or drivers of the price or cost of the offering in units that are useful for the customers' planning and consumption management. User-defined Cost Drivers must not contain spaces so they can be used in Portfolio Designer formulas.
Objectives	The Objectives list is used to configure Objective Metrics that are available in a drop-down list when creating Objectives in Objective Manager for Service Offerings.
Unit of Measure	Units of Measure are used in conjunction with Metrics to configure Objectives in Objective Manager for Service Offerings.
Business Goals and Initiatives	The Business Goals and Initiatives list is used to configure four types of reporting classifications used by Service Offerings: Business Category, Internal, Business Process and Business Initiative.
Language	The Language list is used to manage the list of languages that are available for users to select in the Preferred Language drop-down list in the user's profile and in the person information. For more information, see the "Language" section on page 3-7.
Offering Attributes	Attributes allow service offerings to be described relative to how well they support business initiatives and processes.

Business Goals and Initiatives

Portfolio designers will use Portfolio Designer to associate business initiatives to one or many Service Offerings as a way to link IT work with what matters most to the business. The business initiatives defined here can be associated with a Service Offering via a pop-up window from My Services Executive's Portfolio Optimization tab.



Name	Descriptive name for the initiative. This name appears in the pop-up list of business initiatives in Portfolio Designer where you associate them with service offerings.
Description	Description of the business initiative in more detail.

Status	Set the status by clicking either **Deactivate** or **Reactivate** at the bottom of the page. You may select an **Active** business initiative on the Attributes page in Portfolio Designer when creating or editing a Service Offering. **Inactive** business initiatives are unavailable for selection. You cannot delete business initiatives; you may only activate or deactivate them.
Start Date	Start date for the business initiative.
End Date	End date for the business initiative. This information appears as part of the business initiative details popup window when a user clicks a business initiative name from My Services Executive's Portfolio Optimization tab.
Revenue Impact	Revenue impact figure in terms of dollars over the entire year.
Priority	Priority for the business initiative.

Language

The My Services module is available in multiple languages. The Language list is used to manage the list of languages which are available for users to select in the Preferred Language drop-down list in their Person Profile (see the "Preferred Language" section on page 2-2). By default, only US English is available in the Preferred Language drop-down list. Other languages can be made available by adding them to the Language List. Click **Add**, select the language from the drop-down list, and then click **Update**. No additional configuration steps are required.

For My Services, the supported languages are as follows:

- US English
- German
- French
- Spanish
- Dutch]
- Chinese (Simplified)
- Chinese (Traditional)
- Brazilian-Portuguese
- Japanese
- Korean

For all other modules, the only language supported is US English.

Offering Attributes

You may create an unlimited number of attributes. (No attributes are preconfigured.) Later, you can associate them with service offerings. Create attributes that will allow you to describe offerings relative to how well they support business initiatives and processes. Offering attributes appear in a drop-down list in Portfolio Designer where you associate them with service offerings. See the Portfolio Designer online help for more information.

Site Settings

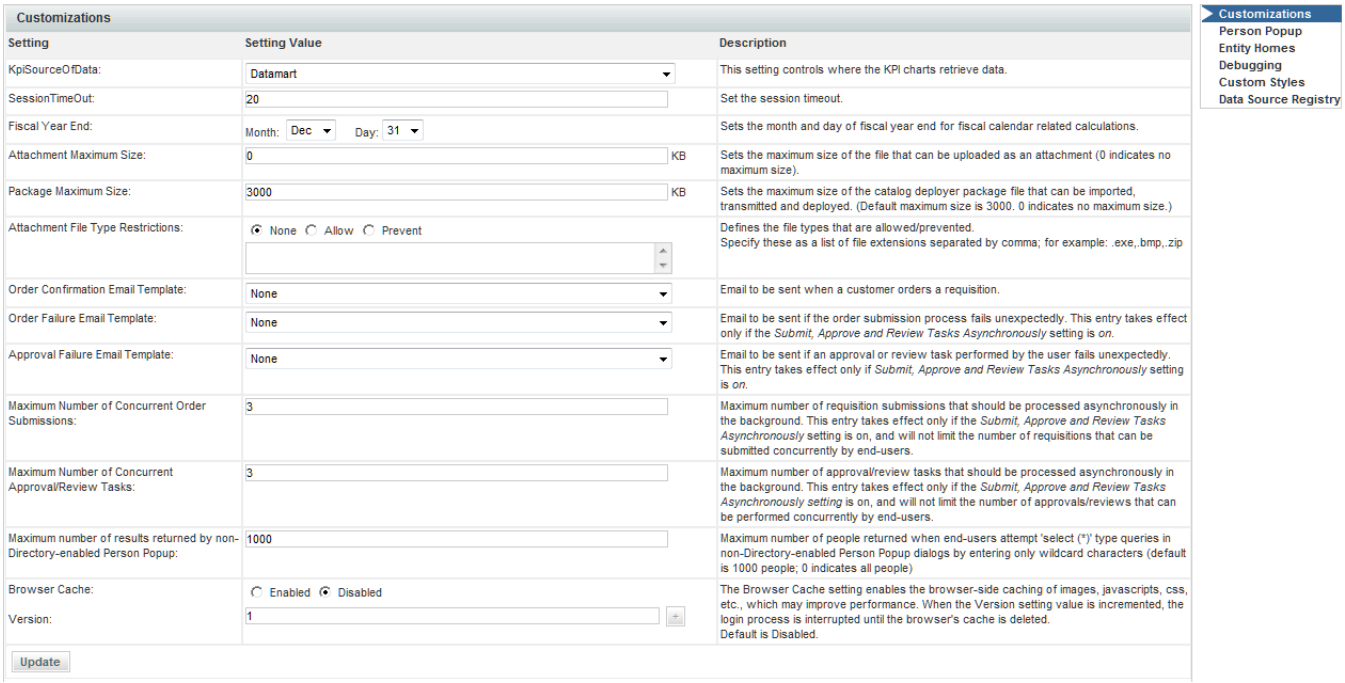
Administration allows you to customize a variety of behaviors to suit the policies and working practices of your organization. You can set these options by clicking the Settings tab. The Settings tab displays the following options:

Page	Description
Customizations	Configure site-wide settings for various modules.
Person Popup	Set the type of information that displays when conducting a person search.
Entity Homes	Specify the definitional data that can be modified on the sites of an implementation.
Debugging	Specify whether to display debugging information within the user interface.
Custom Styles	Define custom styles and specify the organization(s) to which they apply.
Data Source Registry	View the data sources registered with the application.

Customizations

Customizations allow you to set options according to the business practices of your organization.

The Customizations settings are divided into groups depending on the module or modules affected and the capabilities provided by each setting.



The following values are available for customization:

KpiSourceOfData	Controls where the KPI charts retrieve data. Should be set to “Datamart”.
SessionTimeOut	Sets the session timeout; default is 20 minutes; may be any interval up to two hours (240 minutes).
Fiscal Year End	Sets the month and day of fiscal year end for fiscal calendar related calculations used by Demand Center.
Attachment Maximum Size	Sets the maximum size of the file that can be uploaded as an attachment to a service request. 0 indicates no maximum size.
Attachment File Type Restrictions	Defines the file types that are allowed/prevented from being attached. Specify these as a list of file extensions separated by comma; for example: .exe, .bmp, or .zip.
Order Confirmation Email Template	E-mail notification to be sent when a customer submits a requisition.

Asynchronous Submission/Last Approval

In order for Request Center to process a service request, it must create a series of records in the transactional database corresponding to the authorization and delivery tasks that comprise the service’s workflow. For complex delivery plans, creating these tasks and computing the scheduled start and end dates of all tasks, based on the participants assigned, their work calendars and the specified task duration, may consume a substantial amount of time, during which the user (whether the requestor or the last approval) must sit and wait for acknowledgement that their attempt to submit the service request has been processed.

To eliminate this wait time, Service Portal provides the option to implement asynchronous task instantiation. That is, when the request is submitted (or last approval completed, if the request has any authorizations or reviews), Service Portal will only update (or create) the service request itself before allowing the user to continue. The remaining processing—of creating the tasks and computing due dates—will be performed asynchronously, in the background.

This results in one major change in the user interface (elimination of the wait time!) and some minor changes. In particular, the status of the requisition may not be immediately updated; the user may have to refresh the screen for updated details to appear.

In the rare case when Service Portal encounters an error in creating all the tasks, a notification email can be sent to concerned parties. Two email templates can be designated: one for use if a request fails to be submitted, and the second if the last approval fails to be processed correctly. Templates are designed using the Notifications option in the Administration module and associated with each event via the Administration à Customizations settings. Failed requests can be viewed and sent for retry on the Administration Debugging page. See the “Monitor for Asynchronous Submission Messages” section on page 3-21 for more details.

Asynchronous task instantiation is off by default. You must activate this behavior by turning on the “Submit, Approve and Review Asynchronously” setting in the Common section of the Administration Settings.

Order Failure Email Template	E-mail to be sent if the order submission process fails unexpectedly. This entry takes effect only if the Submit, Approve and Review Tasks Asynchronously setting is **on**.
Approval Failure Email Template	E-mail to be sent if an approval or review task performed by the user fails unexpectedly. This entry takes effect only if Submit, Approve and Review Tasks Asynchronously setting is **on**.

Maximum Number of Concurrent Order Submissions	Maximum number of requisition submissions that should be processed asynchronously in the background. This entry takes effect only if the Submit, Approve and Review Tasks Asynchronously setting is **on**, and will not limit the number of requisitions that can be submitted concurrently by end-users.
Maximum Number of Concurrent Approval/Review Tasks	Maximum number of approval/review tasks that should be processed asynchronously in the background. This entry takes effect only if the Submit, Approve and Review Tasks Asynchronously setting is **on**, and will not limit the number of approvals/reviews that can be performed concurrently by end-users.

Browser Cache Setting

This setting enables the use of browser caching for application files that are mostly static in a production environment. Use of this feature could significantly improve page load times for users in remote locations by leveraging cached objects and prompting refresh only when version changes are detected.

When browser caching is enabled, a cookie is placed in the browser client to track the last accessed version, and allow the application to make use of the cached version of the following types of objects:

- Images (*.gif, *.jpg, *.png, *.bmp)
- The CF Image Servlet (presentation-attachment.cfm) used by Request Center to display images associated with categories and services
- Stylesheets (*.css)
- ISF libraries (*.js and *.cfm deployed under RequestCenter.war; this does not include Javascripts generated on the fly by streamJS.jsStream for conditional rules, and user-defined JavaScripts)
- HTML (*.html, *.htm) pages

When an application change event happens (for example, deploying a service with modified images through Catalog Deployer), administrators can prompt users to delete their browser cache by incrementing the version number.

Users who have browser cookies registering a different version from the one in the Administration Settings will be prompted to delete the browser cache. Once the browser cache has been deleted, they can click the “Login Again” button (or “Continue” button, when Single Sign-On is enabled) to access the application.

Common Settings

The Common Settings affect the behavior of multiple modules.

Enable Custom Header Footer	Enable custom header and footer. Default is off.
Enable Custom Style Sheets	Use a custom stylesheet for formatting the site, allowing for the changing of logos, color schemes, fonts and other HTML attributes. Default is off.
Directory Integration	Enable the Directories feature that searches for and imports users into the site from an external datasource. Default is off.

Restrict Site Administrator URL	Allow only those users with the Site Administrator role to log in using the administrative URL to bypass Single Sign-On. Default is off.
Remember Password	Enable or disable the “Remember Me” functionality on the login page. Default is on.
Show “Sign Me Up”	Show or hide the “Sign Me Up” link on the login page. Default is off.
Show “Forgot Password”	Show or hide the “Forgot Password” link on the login page. Default is off.
Use Image Path Replacement	Use a dynamic variable in place of the server portion of presentation image URLs. Default is off.
Use Strong Encryption	Use strong encryption for form data and document attachments. Use is not recommended. Default is off.
Show KPI Portlet	Turn the Key Performance Indicators (KPI) portlet feature on or off. If the feature is on, users who can run My Services Executive will be able to see KPIs on their My Services home page. KPIs are always viewable in the Reporting dashboard for users with permissions to access the Reporting module. Default is off.
Submit, Approve, and Review Asynchronously	Enable or disable background processing of requisition submit, and of completion of approvals and reviews. Default is off.
Deploy Entries (data) in Standards Tables	Enable or disable the inclusion of entries (data) from Standards tables, in addition to the definition of those tables, when creating Catalog Deployer packages. Leave this Off if you do not wish to have Standards data overwritten by a package deployment. Default is on.
Show Login Name	Show or hide the display of person login name on the view person profile popup page. Default is off.

Style-Related Settings

Turning on custom style sheets and/or headers and footers is just the first step to configuring a customized appearance for the web pages. Administrators need to design the styles to be used, upload appropriate files to the application server, and use the Custom Styles option of Administration to associate styles with the site or with specific organizations within the site.

Directory Integration-Related Settings

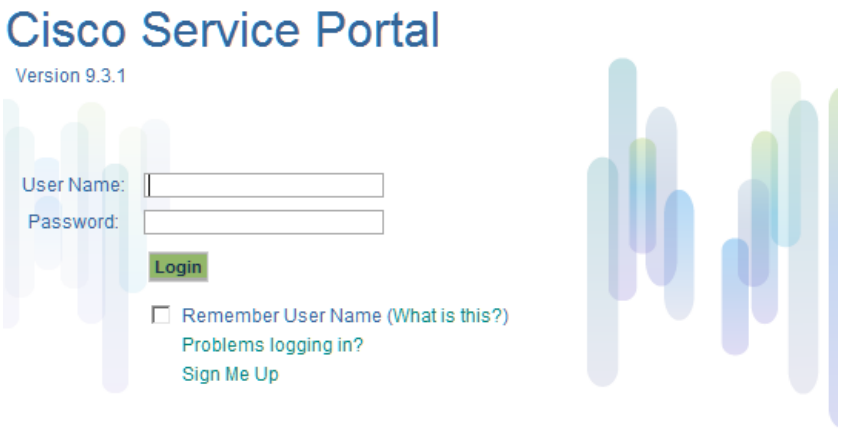
Turning on directory integration is just the first step to integrating Service Portal with an enterprise LDAP directory, which provides personnel (person and organization) data for use in Service Portal, as well as external authentication against that directory and Single Sign-On capability. Directory integration can temporarily be turned off by changing this setting to "Off".

Directory integration configuration includes the ability to override external authentication or Single Sign-On, for troubleshooting, testing, or other reasons. This administrative override should typically be restricted to users who have Site Administrator privileges.

For details on directory integration, please see the *Cisco Service Portal Integration Guide*.

Login-Related Settings

When the default settings regarding passwords and the login are in effective, the Login window looks like this:



That is, the "Remember Password" prompt is shown, but the "Sign Me Up" and "Forgot Password" prompts are not. These settings are not relevant for installations that use Single Sign-On (configured via Directory Integration) to bypass the login screen.

Catalog Deployer-Related Settings

When Catalog Deployer deploys a service, the definitions of any standards referenced by that service (typically in the form of data retrieval rules) are automatically deployed and entries (data) for those standards are also deployed. The setting to "Deploy Entries (data) in Standards Tables" allows you to override that behavior. If set to "No", Catalog Deployer does not deploy standards data to the target environment. It is assumed that data will be loaded into the target environment via alternate methods, either through manual entry using Lifecycle Center or by importing the standards data.

For more information, please see the *Cisco Service Portal Designer Guide*.

My Services Settings

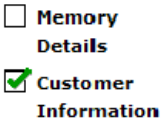
The My Services settings control the behavior and appearance of the My Services module of Request Center.

Show Plan In My Services	Allow customers to see the status of tasks in the delivery plan for their requested services. Default is off.
Allow Update Quantity	Allow My Services users to update the quantity for service requests. Default is off.
Use Categories In Search	Include category names in the My Services search feature. Services contained within matching categories will be displayed in the search results. Default is on.
Display Empty Category	Show or hide categories that do not contain services in the My Services portal. Default is off.
Hide Form Monitor	Show or hide the Service Form dictionary monitor. Default is off.
View Authorization Portlet	Turn the My Services Authorization portlet feature on or off. When enabled, all users will see the Authorization portlet. This setting can be overridden by the corresponding setting in each user's Profile. Default is on.
View Service Items Portlet	Turn the My Services Service Items portlet feature on or off. When enabled, all users will see the Service Items portlet unless they turn it off in their profile. Default is off.
View Common Tasks Portlet	Turn the My Services Common Tasks portlet feature on or off. When enabled, all users will see the Common Tasks portlet. Default is on.
View Requisitions Portlet	Turn the My Services Requisitions portlet feature on or off. When enabled, all users will see the Requisitions portlet. Default is on.
Allow Order On Behalf For All Users	Grant access to Order on Behalf feature for all users. This setting is provided for backward compatible with previous versions of Service Portal. It should not be used. We strongly recommend granting Order on Behalf permission through roles instead. Default is off.

Show All Users For Order On Behalf	Allow the person using the Order on Behalf of feature to order services for any user in the site, regardless of organizational unit- or person-specific Order on Behalf permission settings. Default is off.
Open Authorization Task in a popup	When enabled, Authorization tasks in My Services will open in a different popup window. Default is off.

Form Monitor

The Form Monitor is displayed to the right of a service form. It shows the dictionaries in the form. A dictionary is checked when all mandatory fields in that dictionary have been provided values.



The Form Monitor is generally useful. However, it may be confusing if a dictionary is hidden by a rule or ISF code after the service form has been displayed; the dictionary will still be listed in the Form Monitor.

Authorizations Portlet

The Authorizations Portlet provides a quick way to view and access any authorizations assigned to the current user. If users are able to view their authorizations this portlet is displayed on the left side of the My Services screen.

The Authorizations Portlet provides a quick view of the five most recent authorizations and a means of displaying all authorizations assigned to the current user. Authorizations are also accessible via the **Common Tasks > Authorizations** link and the Authorizations tab in the navigation bar of the My Services module.

Service Items Portlet

The Service Items Portlet provides a quick way to view and access any service items assigned to the current user. This portlet is available only for sites that have licensed Lifecycle Center.

The Service items Portlet provides a quick view of the five most recently provisioned service items and a means of displaying all service items assigned to the current user. Service Items are also accessible via the Service Items tab in the navigation bar of the My Services module.

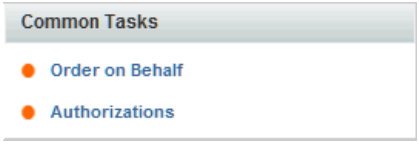
Requisitions Portlet

The Requisitions Portlet provides a quick way to view and access the five most recently submitted ongoing requisitions. When enabled, this portlet is displayed on the left side of the My Services screen.

Requisitions are also accessible via the Requisitions tab in the navigation bar of the My Services module.

Common Tasks Portlet

The Common Tasks Portlet provides short cuts to commonly used My Services actions. When enabled, this portlet is displayed on the left side of the My Services screen.



My Services Portlets

The My Services portlets (for Authorizations, Service Items, Requisitions, and Common Tasks) are pre-configured. All, some or none can optionally be displayed on the left side of the My Services home page. If no My Services portlets are displayed, the content portion of the page (the Service Catalog) expands to take up the entire width of the page.

The My Services portlets are preconfigured to have the content and appearance described above. If you would like to further customize the use and/or appearance of portlets, you may do so using the Cisco Portal Manager, described in the *Cisco Service Portal Designer Guide*.

Service Manager Settings

Service Manager settings affect the appearance and behavior of the Request Center Service Manager module.

Show Task Link	When displaying delivery process tasks, include a hyperlink on all of the tasks, allowing the user to quickly jump to other tasks in the plan. Default is on.
Related Tasks Default To Wait	When creating Ad-Hoc Tasks, set the option to pause the current task. This can still be overridden at the moment of creating the Ad-Hoc Task. Default is off.
Enable Ad-Hoc Task Email	When enabled, Request Center will automatically send the "Ad-Hoc Task Started" notification email to the performer of any new Ad-Hoc Task created. Default is on.
Show Undefined Roles	In the staffing section of monitor tasks, display roles that have not been defined in the service delivery plan. Default is off.
Service Performers Can Search All Performers	When enabled, users can search for all other people with access to Service Manager in the Performer search feature. Otherwise, users are restricted to just those people that are in their service teams. Default is off.
Allow Task Supervisors To Cancel Tasks	Allow task supervisors to cancel or skip the delivery tasks that they are assigned to supervise for the service. Default is off.
Enable completion of external tasks	Enable the display and completion of external tasks in Ongoing status in Service Manager. Such tasks are typically shown only in the Service Link module's View Transactions. This setting applies to all external tasks that are added to a delivery plan while the setting is enabled. Those tasks will still be available for completion in Service Manager even if the setting is disabled afterwards. The system administrator should keep the setting consistent. Default is off.
Show Bundle Data	Display a composite order form of all dictionaries on the Data page for a bundled service when on any task within the service. When disabled, only those dictionaries for the selected included service will display. Default is on.
Open Task in a popup	When enabled, Tasks in Service Manager will open in a different popup window. This allows users to have a primary window that shows the task list and a secondary window that displays the details of tasks selected. The task list is refreshed when the Refresh button is clicked or when the page is reloaded. Reducing the frequency of the task list refresh places less load on the application and helps to improve overall application performance. Default is off.

Demand Center Settings

The Demand Center settings control the behavior and appearance of Demand Center.

Enable Service Offering Catalog	Allow for creating a Service Offering Catalog for Portfolio Center in the Categories component of Service Designer. Default is off.
Enable Agreement Management	Enable Agreement Management functionality in the My Services Executive and Relationship Manager modules. Default is off.
Enable Ordering Permission	Enabling this property will provide ordering permissions for Included services in Request Center. Default is off.

Service Link Setting

The Compress Messages setting controls whether Service Link messages (both the internal nsXML message and the external message) are compressed when they are held in the repository. Since the internal nsXML message can be quite large, compression is recommended. Other means to reduce the amount of storage required for Service Link messages are to configure the agent to minimize message content and/or to periodically purge messages for completed tasks. These options are explained in the *Cisco Service Portal Designer Guide*.

Compress Messages	Messages in the database will be compressed when this flag is turned on. Messages will use less space, but will not be easily read by the human eye. Default is on.

Web Services Setting

The Enable Web services setting controls whether web services for requisitions, tasks or service offering operations are accepted. The setting does not apply to the Service Link http/web service adapter.

Enable Web services	Enabling this property will provide access to Web services. Default is off.

Custom Styles

The appearance of customer-facing modules in the application can be customized using Cascading Style Sheets (css) and custom headers and/or footers. Cascading Style Sheets offer the ability to customize the appearance of web pages by changing the definition of styles used to display the pages, rather than having to edit the pages themselves.

The pages which may be customized include:

- Pages displayed in the Request Center My Services and Service Manager modules, including service forms dynamically generated based on definitions specified via Request Center Service Designer
- Pages displayed in the Demand Center modules Relationship Manager, My Services Executive, and Service Level Manager

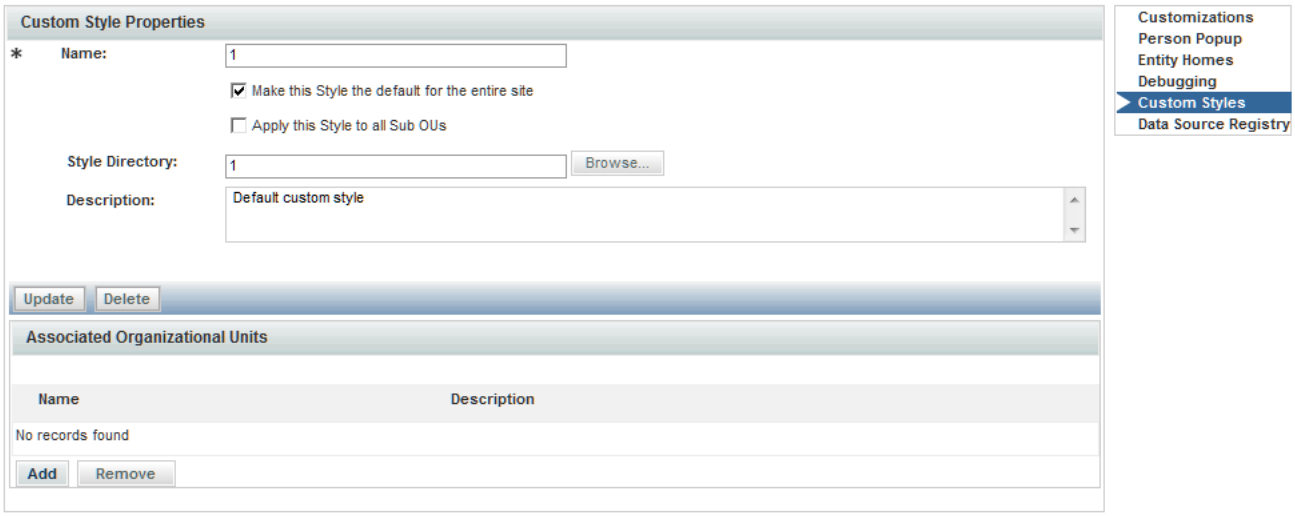
- The pages for Reporting and Advanced Reporting
- The modules that are defined using Portal Manager
- The login pages

The appearance of modules used by service designers and administrators to configure and manage Service Portal cannot be customized. These modules include Service Designer, Organization Designer, Portfolio Designer, Administration, Catalog Deployer, Service Item Manager and Service Link.

Designers can reference Chapter 4, "Custom Style Sheets" for more detailed information.

Defining a Custom Style

The Custom Styles page is used to define a style and specify the organization(s) to which it applies.



Fill in the properties as follows:

Name	The style name should reflect the installation name or the organization(s) to which the styles will apply.
Make this Style the default for the entire site	One style may be designated as the default. If a default is specified, it will be used for any user whose home organization (OU) has not been assigned a style. If no default is specified, the system-defined style sheets will be used.
Apply this Style to all sub OUs	If a hierarchical structure is used in the organizations, you may specify that a style is inherited by all child OUs of a parent.
Style Directory	You may select the Style Directory from any directory under RequestCenter.war\custom. The directory must exist before you can create the style. The default, a directory named 1, already exists.

You may edit the style definition or the business units to which it applies at any time.

Enabling Custom Style Sheets and Headers/Footers

Select the Administration module and go to the Settings tab. The Customizations page is displayed. The Common settings include parameters to “Enable Custom Header Footer” and “Enable Custom Style Sheets,” as shown below.

On	Off	Setting	Description
Common			
○	◉	Enable Custom Header Footer	Site will add content from the custom header and footer HTML. Default is off.
○	◉	Enable Custom Style Sheets	Site will utilize the custom stylesheet allowing for the changing of logos, color schemes, fonts and others. Default is off.
○	◉	Directory Integration	Enable the Directories feature that searches for and imports users into the site from an external datasource (e.g. LDAP). Default is off.
○	◉	Restrict Site Administrator URL	Allow only those users with the Site Administrator Role to log in using the administrator URL (i.e., bypassing Single Sign-On). Default is off.
◉	○	Remember Password Enabled	Enable or disable Remember Me functionality on the login page. Default is on.
○	◉	Show "Sign Me Up"	Show or hide the "Sign Me Up" link on the login page. Default is off.
○	◉	Show "Forgot Password"	Show or hide the "Forgot Password" link on the login page. Default is off.
○	◉	Use Image Path Replacement	Use a dynamic variable in place of the server portion of presentation image URLs. Default is off.
○	◉	Use Strong Encryption	Use strong encryption for form data and document attachments. Default is off.
○	◉	Show KPI Portlet	Turns the Key Performance Indicators (KPI) portlet feature on or off. Default is off.
◉	○	Submit, Approve, and Review Asynchronously	Enable or disable background processing of requisition submit, and of completion of approvals and reviews. Default is off.
◉	○	Deploy Entries (data) in Standards Tables	Enable or disable the inclusion of entries (data) from Standards tables, in addition to the definition of those tables, when creating Catalog Deployer packages. Leave this Off if you do not wish to have Standards data overwritten by a package deployment. Default is on.
○	◉	Show Login Name	Show or hide the display of person login name on the view person profile popup page. Default is off.

To enable custom stylesheets, change the corresponding parameter setting from “Off” to “On.” Save your changes by updating the page. Any custom styles specified in the custom.css file (in place on the application server) will be in effect.

Similarly, to enable custom headers and footers, change the parameter setting for the “Enable Custom Header Footer” parameter to “On.”

Once you start a session with these parameters turned on, there is no need to exit from your session to view style changes. Once the definition of the style is changed and the file placed on the specified directory of the application server, refreshing the page will use the new style definitions.

The Person Popup

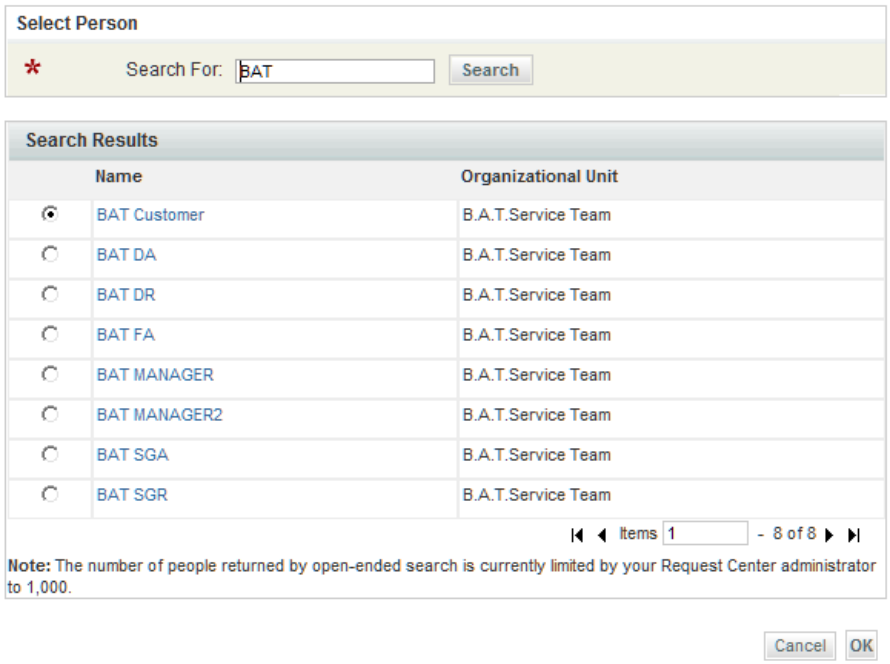
The Person Popup allows you to configure which data appears on the Person Popup window that appears when a user performs a person search. Person searches can be performed in Request Center:

- When ordering on behalf of another person
- When a person-based dictionary or person type field is used in a service form
- When a user selects a temporary authorization delegate

You can specify how you wish the heading to appear and what information populates each field. By default, Name is populated with the string defining the person's first and last name. You can have a maximum of four fields of information about a person.

Any field except Name may be removed from the display by blanking out the Column Heading and corresponding Person Data.

The definition of a Person Popup shown above results in a Person Search pop-up that looks like:



Entity Homes

The Entity Homes feature provides a means to enforce corporate change management policies. In a multi-site implementation (Development, Test and Production), you may decide to isolate where certain entity types may be modified to create a system of record for the entity. This is a common approach for managing content change. For example, you may want to isolate service definition changes to be allowed only on the Development site and use Catalog Deployer and associated tools to promote changes to Production. In this case, the service definition's system of record or “home” is **Development**.

Entity Home Settings are essentially “documentation only” until a site protection level other than “None” is assigned to the site.

Setting	Description
None	No protection is enabled on this site.
Create only	Non-home entities cannot be created on this site.

Create, Modify	Non-home entities cannot be created or modified on this site.
Create, Modify, Delete	Non-home entities cannot be created, modified, or deleted on this site.

The site protection levels govern the appearance and behavior of the pages in Service Designer or Organization Designer that allow users to modify entities. They override any capabilities or permissions that have been granted to a user via roles or direct permission assignments. For example, if the user has the capability to manage service definitions in a site, but the Entity Home setting for service definitions does not allow updates on the site, the user will not be able to make any changes.

Together, Entity Homes and the Catalog Deployer module allow you to establish a change management process and policy that meets your business requirements. For details instructions on setting up Entity Homes and using Catalog Deployer, please consult the *Cisco Service Portal Designer Guide*.

Debugging Settings

Common Settings

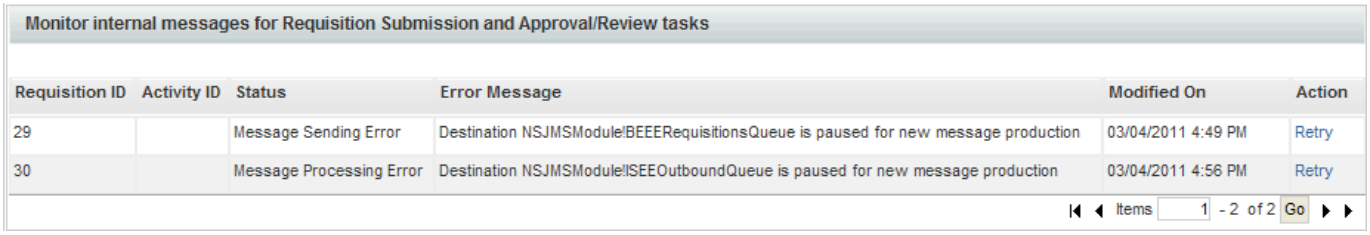
The settings on the Debugging option allow you to configure the system to display debugging information that can help diagnose problems and provide help to the Cisco Technical Assistance Center (TAC).

Turning on a "Debug" setting displays additional information on the standard screens. These settings are typically used only when working on a development or QA installation or temporarily in a production instance, to gather details on a previously noted problem. For more information, please see the *Cisco Service Portal Configuration Guide*.

Setting	Description
Debug	Turns on the display of basic debugging information to the user, including the URL and parameters of the current page and, in case of an error, a stack trace.
DebugCfx	Turns on the display of ColdFusion debugging information.
Directory Map Testing	Enables testing of a mapping used by directory integration. For more information please see the *Cisco Service Portal Integration Guide*.

Monitor for Asynchronous Submission Messages

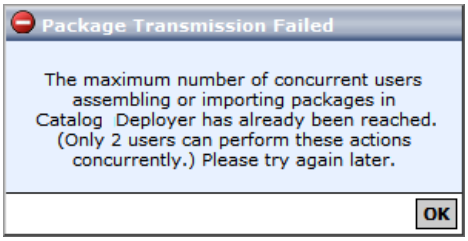
The message monitor is used only when the Submit, Approve and Review Tasks Asynchronously setting is on. In the rare case when Service Portal encounters an error in processing a requisition submission or task authorization request asynchronously, the failed messages are displayed in the internal messages monitor section.



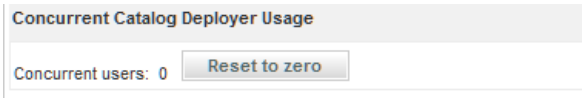
You can rectify the underlying issues based on the error message shown, and resume the processing of the failed messages by clicking **Retry**.

Catalog Deployer User Counter Reset

This setting allows you to reset the number of concurrent Catalog Deployer users to zero. The maximum allowable number of concurrent Catalog Deployer users is two. If there are more than two concurrent Catalog Deployer users, a message describing the condition appears, for example:



You may occasionally encounter this message even if one or both of these Catalog Deployer users have finished all deployment operations. In other words, this message may appear erroneously after concurrent Catalog Deployer usage. If you see the above error message while using Catalog Deployer and you know it to be erroneous, a user with Site Administration privileges can use the utility as shown below to reset the user counter.



Data Source Registry

A data source defines the relational databases from which Service Portal may access information. By default, Service Portal instances have two data sources, one for accessing the transactional data, and a second for accessing the data marts and reporting options.

In addition, administrators may create additional data sources to support components including external dictionaries, SQL options lists, and active form data retrieval rules.

The Data Source registry lists all data sources available. To create a datasource, please refer to the *Cisco Service Portal Installation Guide*.

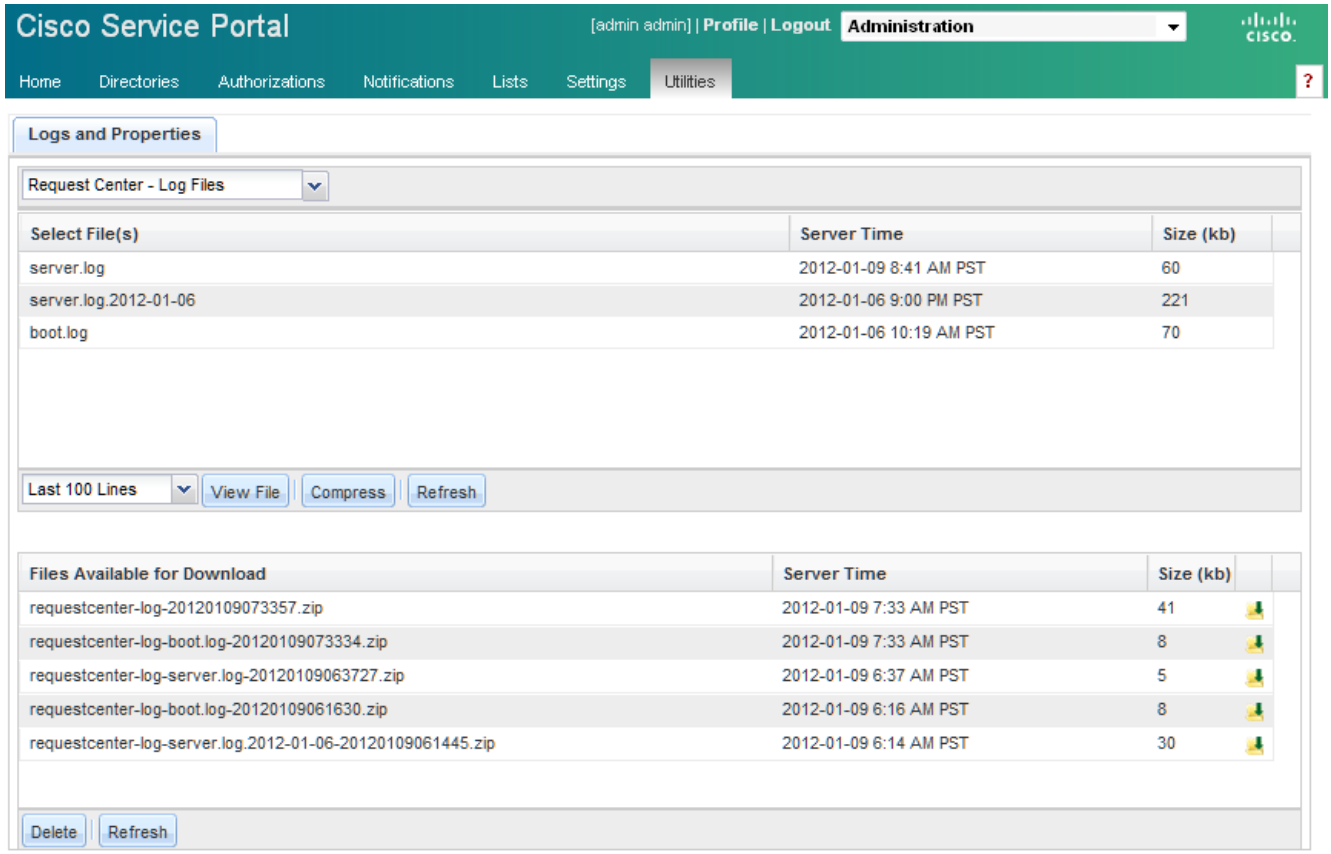
Support Utilities

Administration allows you to view and copy system log and property files for troubleshooting.

You can access the files using one of the following methods:

- On the Home page, click **Use Support Utilities**.
- On the navigation bar, click **Utilities**.

The Logs and Properties tab page appears as shown below.



Note In order to use Support Utilities, both the **Use Support Utilities** and **Access Logs and Property Files** capabilities must be enabled for the user (see the "Capabilities for Administration" section on page 1-42).

Log and Destination Folder Settings

To use the Support Utilities function, the application server's log folder needs to be specified. Also a destination folder needs to be created and specified to store the compressed Zip files (containing the log and property files) until you copy and delete them. You can create and specify a different destination folder for each file type.

Follow the steps below to specify the destination and log folders:

Step 1 Create a new destination folder (or destination folders for each file type). These folders can be anywhere.

Step 2 The destination folder(s) location and maximum size are specified in a **support.properties** file. There are two support.properties files—one for Request Center and one for Service Link.

These support.properties files are located in the following deployed directories:

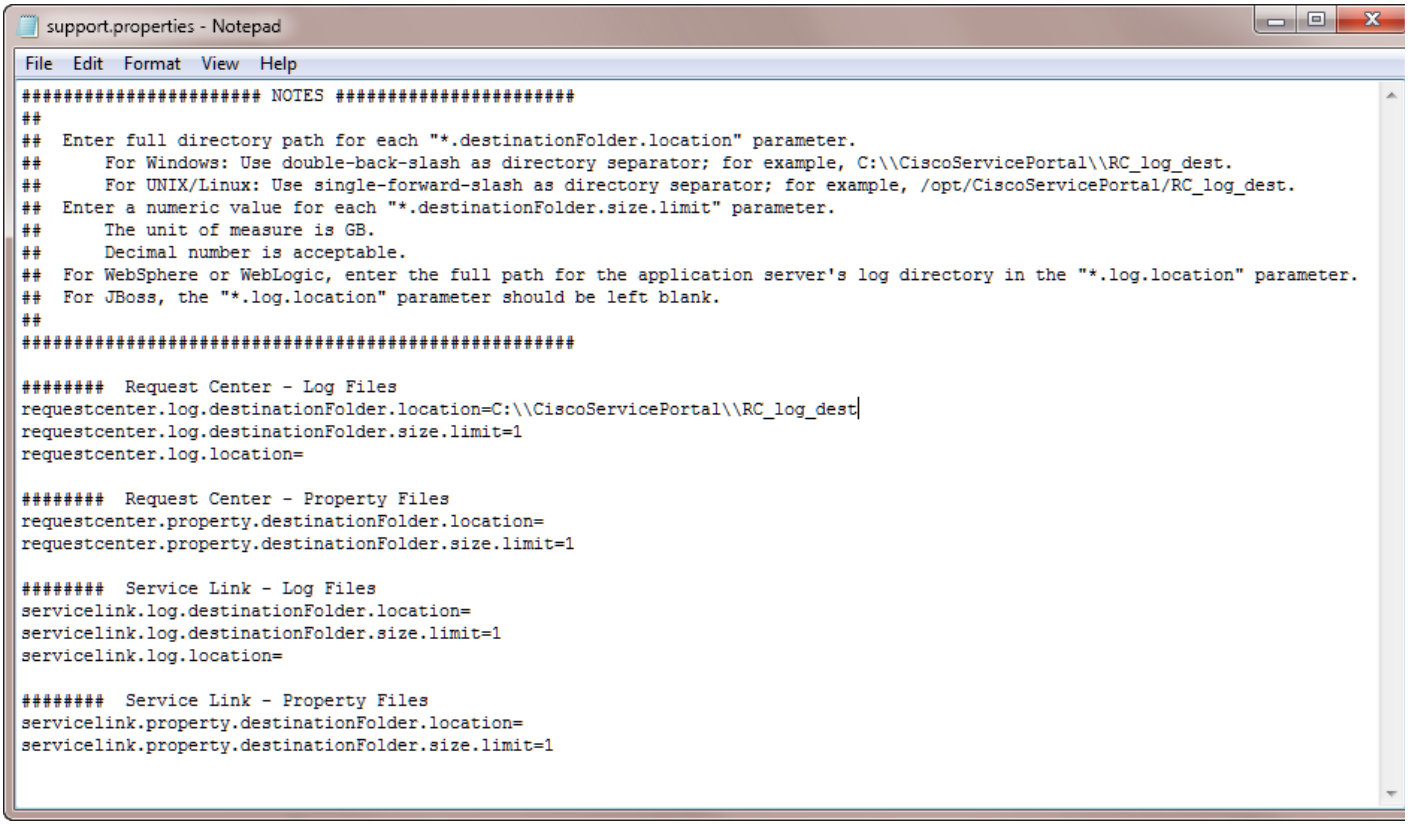
- Request Center: RequestCenter.ear\config\
- Service Link: ISEE.war\WEB-INF\classes\

Note The paths above are for a Windows environment.

Open the support.properties file in a text editor.

An example support.properties file in a Windows environment is shown below.

Note For the Request Center support.properties file, only the Request Center entries are used; the Service Link entries are ignored. For the Service Link support.properties file, only the Service Link entries are used; the Request Center entries are ignored.



Step 3 Enter the full directory path of the destination folder(s) for the “*.destinationFolder.location” parameter. For Windows: Use a double-back-slash as a directory separator; for example, C:\\CiscoServicePortal\\RC_log_dest. For UNIX/Linux: Use a single-forward-slash as a directory separator; for example, /opt/CiscoServicePortal/RC_log_dest.

In the example above,

"C:\\CiscoServicePortal\\RC_log_dest" is set as the location of the destination folder for the Request Center log files.

Step 4 For WebSphere or WebLogic servers, enter the full directory path of the application server's log directory in the "*.log.location" parameter. For JBoss, the "*.log.location" parameter should be left blank.

Step 5 Set the maximum size of the destination folder(s) in the "*.destinationFolder.size.limit" parameter. The unit for the destination folder maximum size is GB. Fractions can be used. For example, if you want to use 500 MB, enter 0.5; for 250 MB, enter 0.25. If the files in this folder exceed this size an error message will be displayed.

In the example above,

1 sets the maximum size of the destination folder to 1 GB.

Step 6 Save the support.properties file.

Step 7 Reboot the Service Portal server.

View and Download Files

To view and download files, follow the steps below:

Step 1 On the Logs and Properties tab page, select a file type from the drop-down menu on the top left.

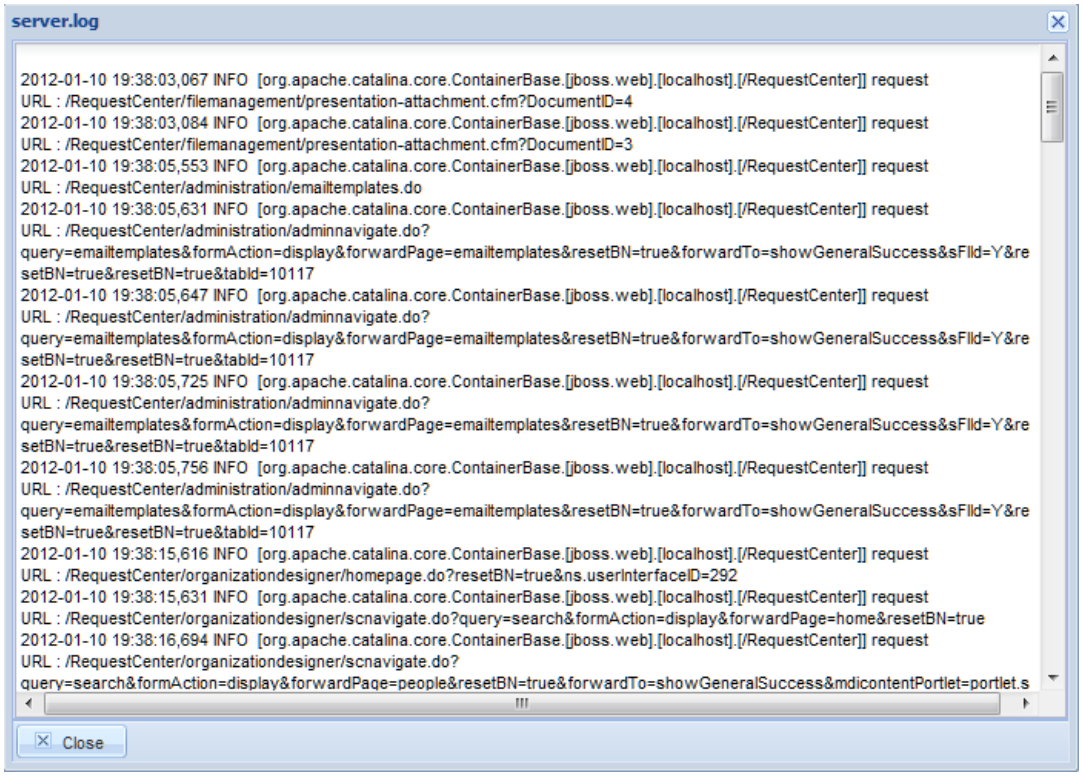
Four types of files can be selected:

- Request Center – Log Files
- Service Link – Log Files
- Request Center – Property Files
- Service Link – Property Files

Step 2 Click on a file in the top panel to select it. If needed, click **Refresh** to see the latest files.

Step 3 To view a file, select the number of last lines to view by selecting the number from the drop-down menu on the bottom of the top panel, and then click **View**.

Step 4 The file opens in a pop-up window. A sample log file is shown below:



Step 5 Click **Close** to close the window.

Step 6 To download one or more selected files (**Ctrl-Click** to select multiple files) to a location of your choice, click **Compress**.

Step 7 Click **Refresh** on the bottom panel to see the compressed file(s) in the bottom panel. The file is compressed into the Zip format and a time stamp is added to the name. For multiple selected files, a single Zip file is created (named only from the file type and time stamp) containing all the selected files.

Note If the same file is compressed again, a new file with a different time stamp will be created—it will not overwrite the previously compressed file.

Step 8 Click the Download icon ( ) for a single file on the bottom panel.

Step 9 A File Download dialog appears. Click **Save**.

Step 10 A Save As dialog appears allowing you to save the file to a location of your choice.

Step 11 Navigate to the location you want and click **Save**.

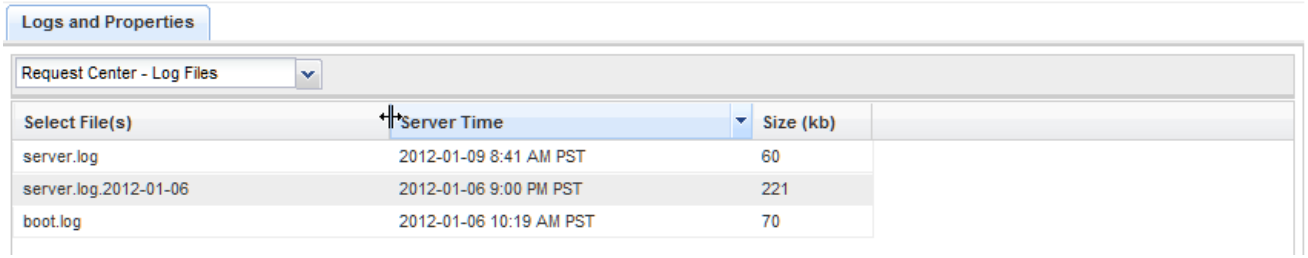
Step 12 After saving the file(s), you can delete selected compressed file(s) (**Ctrl-Click** to select multiple files) from the bottom panel by clicking **Delete**.

Adjusting the Panel Displays

As illustrated below, on the top and bottom panels, you can resize columns, move columns, sort columns, and hide columns.

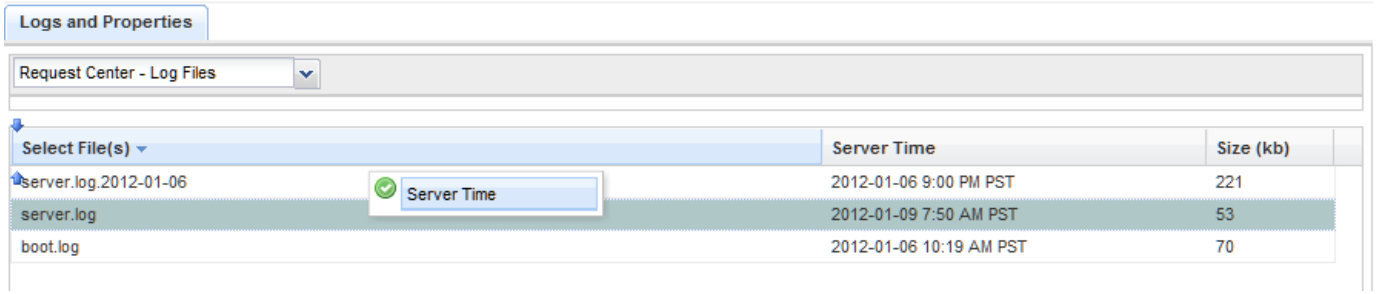
Resizing a Column

Move your mouse between two columns until the Column resize cursor appears ( ). Click and drag it to the desired position.



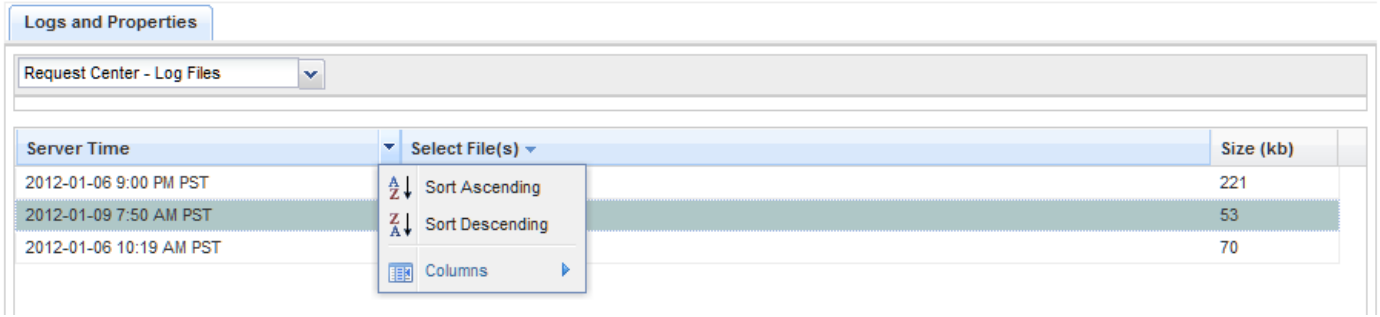
Moving a Column

Grab a column with your mouse and drag it to the desired position. In the example below, the user is dragging the Server Time column to the left.



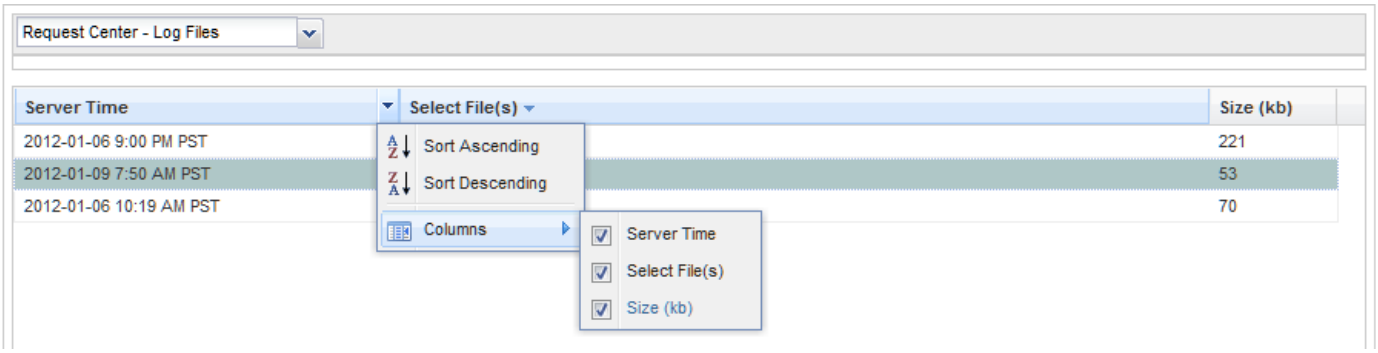
Sorting a Column

Click a column to sort in Ascending order ( ). Click the same column again to sort in Descending order ( ). Alternatively, move your mouse over a column until the Column sort button appears ( ). Click the Column sort button and then select Sort Ascending or Sort Descending.



Hiding or Showing Columns

Move your mouse over a column until the Column sort button appears ( ). Click the Column sort button, select **Columns**, and then use checkmarks to select the columns to display.



CHAPTER 4

Custom Style Sheets

- Overview, page 4-1
- Custom Style Sheets, page 4-2
- Style Summary and Recommended Practices, page 4-13
- Custom Headers and Footers, page 4-20

Overview

This chapter describes the capabilities provided to customize the appearance of the Cisco Service Portal (Service Portal) web pages. This customization is accomplished through the use of Cascading Style Sheets (css) to format those web pages as well as the addition of a custom header and/or footer.

These capabilities allow designers to customize the appearance of all customer-facing modules of Service Portal. The pages which may be customized include:

- Pages displayed in the Request Center My Services and Service Manager modules, including service forms dynamically generated, based on definitions specified via Service Designer
- Pages displayed in the Demand Center modules Relationship Manager, My Services Executive, and Service Level Manager
- The portals for Reporting and Advanced Reporting
- The login pages
- Pre-configured and custom portal pages in the Portal Manager solution

The appearance of modules used by service designers and administrators to configure and manage Service Portal cannot be customized. These modules include Service Item Manager, Service Designer, Organization Designer, Portfolio Designer, Administration, Catalog Deployer, Portal Designer, and Service Link.

Custom Style Sheets

Overview

Contents of the Service Portal application are presented as web pages formatted using HTML. Cascading Style Sheets (css) offer the ability to customize the appearance of web pages by changing the definition of styles used to display the pages, rather than having to edit the pages themselves.

Custom styles allow designers to customize Service Portal web pages, headers and footer. Custom styles may be applied to all users of an application instance, or different styles may be applied to users based on their home organizational unit.

Prerequisites

- You must have access to the file system of the application server, specifically to the "custom" directory of the RequestCenter.war archive and its subdirectories. You need both read and write access to this directory and to its subdirectories.
- You must have a user role which includes the Administration capability to "Manage Global Settings" in order to turn on or off the use of custom style sheets, headers, and footers.
- Browser page caching must be turned off in order for you to test style sheet changes.
- Ideally, you should have access to an application instance where you can test your changes without disturbing the work of other analysts or developers.
- A style sheet editor and other editing tools are highly recommended, but not required.

Customizing Built-in Modules

The procedure below gives the basic steps to follow in order to customize the appearance of styles used in the built-in modules, namely My Services, Service Manager, My Services Executive, Relationship Manager and Reporting. Additional details on these styles are given in the following sections.

1. Create a directory on the application server, under the RequestCenter.war/custom directory, where the files required for the custom styles will reside. The directory will typically have an images subdirectory, for any custom images. The directory name should indicate the tenant/organization name to which the styles will apply.
2. Obtain a copy of the file example.css from the custom/CustomExamples directory of the Service Portal web archive (RequestCenter.war). Location of this archive will vary, based on your application server and installation setting.
3. Name the copied file as custom.css. Change the styles in the custom.css file according to the guidelines given in the next section of this document.
4. Copy the customized file(s) to the new directory you created in Step 1, along with any images referenced in the custom.css.
5. Use the Custom Styles page in the Administration module to define the style, specify the directory on which required files reside, and assign the organization(s) to which the style applies.
6. Use the Settings page in the Administration module to turn on custom stylesheets.

7. Restart the browser session of Service Portal—the pages should be displayed with the customizations applicable to the logged in user. You must exit and restart the Service Portal session when custom stylesheets are initially activated. To test subsequent changes to the styles, it is sufficient to copy the revised style sheet to the application server and refresh the current page. The new styles will be applied, provided page caching is not in effect.

Caution Once you change the Administration Settings to use custom stylesheets, the custom.css file should be present on the specified directory. If the file is not present, Service Portal will use its standard styles. Similarly, if the option to use a custom header or footer is turned on, the corresponding files must be present on the specified directory.

Customizing User-defined Portals

Just like My Services and other built-in modules, the Portal Manager modules can be customized for different organizational units through style sheets. The custom styles are maintained in a different style sheet from the other built-in modules to give you greater flexibility in how you present the Portal Manager modules.

The Portal Manager solution also offers different themes that affect the colors of portlets on a portal page. You can allow users to select their own themes, or give this ability only to portal designers. Refer to the *Cisco Service Portal Designer Guide* for more information regarding portal page themes.

The custom stylesheet for Portal Manager is located in the same custom directory as Service Portal and is enabled/disabled along with it.

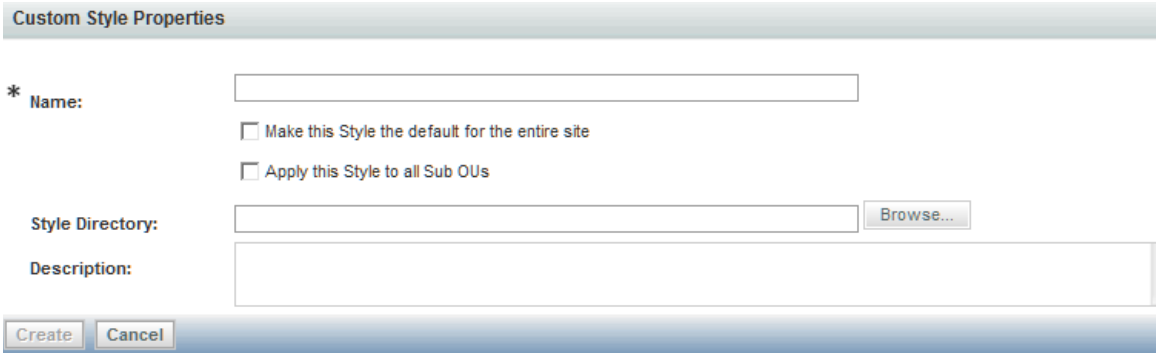
1. Obtain a copy of the file example_portal-custom-header.css from the custom directory of the Service Portal web archive (RequestCenter.war).
2. Name the copied file as portal-custom-header.css. Change the styles in the file according to the guidelines given in the next section of this document.
3. Copy this file into the custom directory created for the tenant/organization (see Customizing Built-in Modules, page 4-2, Step 1) along with any images used.

Defining a Custom Style

To start using custom style sheets or headers and footers:

Step 1 Login to Service Portal, select the **Administration** module, and go to the **Settings** tab. The Customizations page appears.

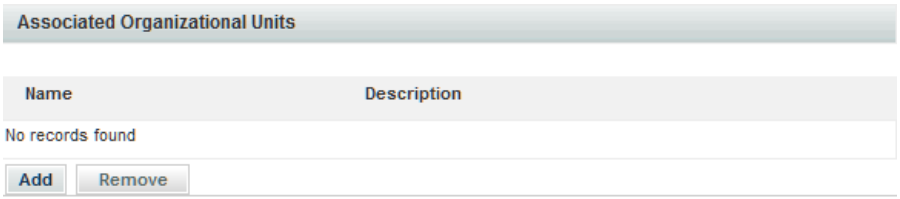
Step 2 Select the **Custom Style** option from the option list at the right side of the screen. Click **Add** to create a new style; the Custom Style Properties page appears.



Step 3 Fill in the properties as follows:

- Style Name should reflect the organization(s) to which the styles will apply.
- One style may be designated as the Default. If a default is specified, it will be used for any user whose home organization (OU) has not be assigned a style. If no default is specified, the default Service Portal style sheets will be used.
- If a hierarchical structure is reflected in the organizations, you may specify that a style is inherited by all child OUs of a parent.
- You may select the Style Directory from any directory under RequestCenter.war/custom. The directory must exist before you can create the style.
- A Description is optional but recommended.

Step 4 Click **Add** to create the style. You can then edit the style, to specify the organization(s) to which the style applies.

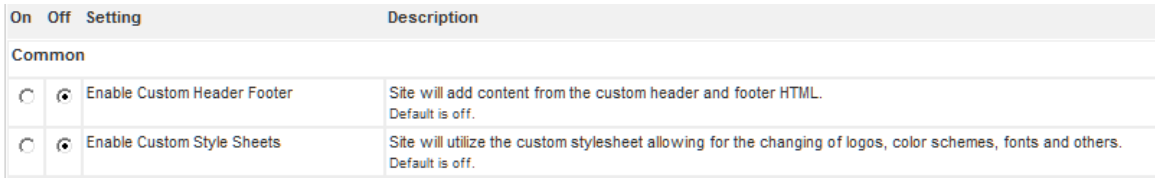


Step 5 Click **Add** in the Associated Organizational Units panel. The Organizational Unit Search window will be displayed. Select one or more business units.

Step 6 You may edit the style definition or the business units to which it applies at any time.

Turning On Custom Style Sheets and Headers/Footers

Select the Administration module, and go to the Settings tab. The Customizations page will be displayed. The Common settings include parameters to “Enable Custom Header Footer” and “Enable Custom Style Sheets”, as shown below.



To enable custom stylesheets, change the corresponding parameter setting from "Off" to the left "On" button. Save your changes by updating the page. When you start a new Service Portal session, any custom styles specified in the custom.css file (in place on the application server) will be in effect.

Similarly, to enable custom headers and footers, change the parameter setting for the "Enable Custom Header Footer" parameter to "On".

Once you start a Service Portal session with these parameters turned on, there is no need to exit from your session to view style changes. Once the definition of the style is changed and the file placed on the specified directory of the application server, refreshing the page will use the new style definitions.

Modifying Customizations with Browser Cache Enabled

If the Browser Cache setting is enabled in the Administration Settings, changes made to custom style sheets, headers and footers will not take effect until the browser cache has been deleted. To prompt the application users to delete their browser cache, follow the instructions in the "Browser Cache Setting" section on page 3-10 to increment the browser cache version.

Customizing Styles

The custom\CustomExamples directory includes files you can use as starting points for customizations of Service Portal. Directory contents are summarized in the table below.

custom (folder) Contents	Description
customExamples	Folder which contains starting points for custom styles, header, and footer
images	Folder which contains the images currently used by Service Portal styles which may be replaced via custom style sheets
common_task_bg.gif	Background for the Common Tasks pane
headerGradient.gif	Background for header styles—style which appear at the top of each portlet or pane
logo_bottom.gif	(Deprecated)
lvl1_nav_shade.gif	Background for the tabs which provide top-level navigation through the options available in each Service Portal module
lvl3_nav_shade.gif	Background for level 3 headers—also recommended for page footers
mark.gif	Denotes a mandatory field on a service form
orange_bullet.gif	Common Tasks bullet
orange_li_bullet.gif	(Not used in example custom.css)
page_footer_shade.gif	Gif available for page footer shading

PopupHeaderGradient.gif	(Not used in example custom.css)
requiredMark.gif	Denotes a mandatory field on all user interface pages other than service forms
tfoot_shade.gif	(Not used in example custom.css)
example.css	Sample file, mirrors default Service Portal settings to start with, with solid color replacing gradients
example_portal-custom-header.css	Sample file, mirrors default Portal Manager header area settings
example_footer.html	Starting point for developing custom footer
example_header.html	Starting point for developing custom header

The CustomExamples/example.css and example_portal-custom-header.css files (the template for your custom.css file) are formatted as a standard cascading style sheet file and includes comments to guide you in selected styles to modify. These comments include brief descriptions of where and how a particular style is used; however, some experimentation will be required to fine tune customizations.

The original definitions for customized styles should be retained as comments in the style sheet. This practice is recommended, in case a customized change needs to be backed out and to maintain traceability to the original page appearance.

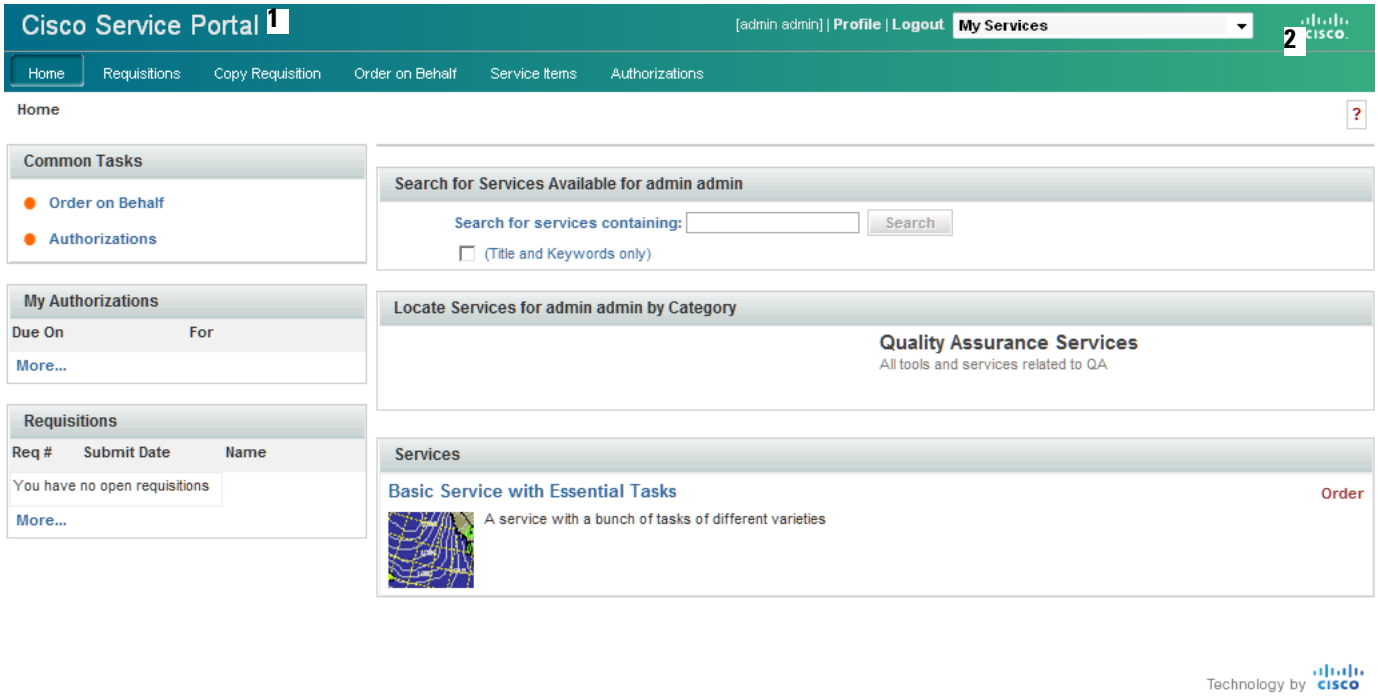
The original custom.css and example_portal-custom-header.css files are shown in the "Custom Headers and Footers" section on page 4-20. (Some minor layout changes from the original have been made to enhance legibility.) Please consult the complete file before applying any changes.

Page Headers

The page header for the end-user facing modules is governed by the following styles:

- lvl1_nav (for built-in modules only): The "Level1 Navigation Bar" provides the background for the application module drop-down menu and menu bar. The application name cannot be modified but can be hidden using the "lvl1_nav_title" style if desired.
- header (for user-defined modules only): The header style is used with portal modules that are created/maintained using Portal Designer. The usage is similar to the lvl1_nav above.
- headerlogo, leftheaderlogo: The two header logo styles provide flexibility in placing the logo at either the left or right hand side of the header, as shown in the examples that follow. When the left logo is used, the background property of the application name must be set to none. The styles governing the application module menu may also be modified so that it can be positioned at the right-hand corner.

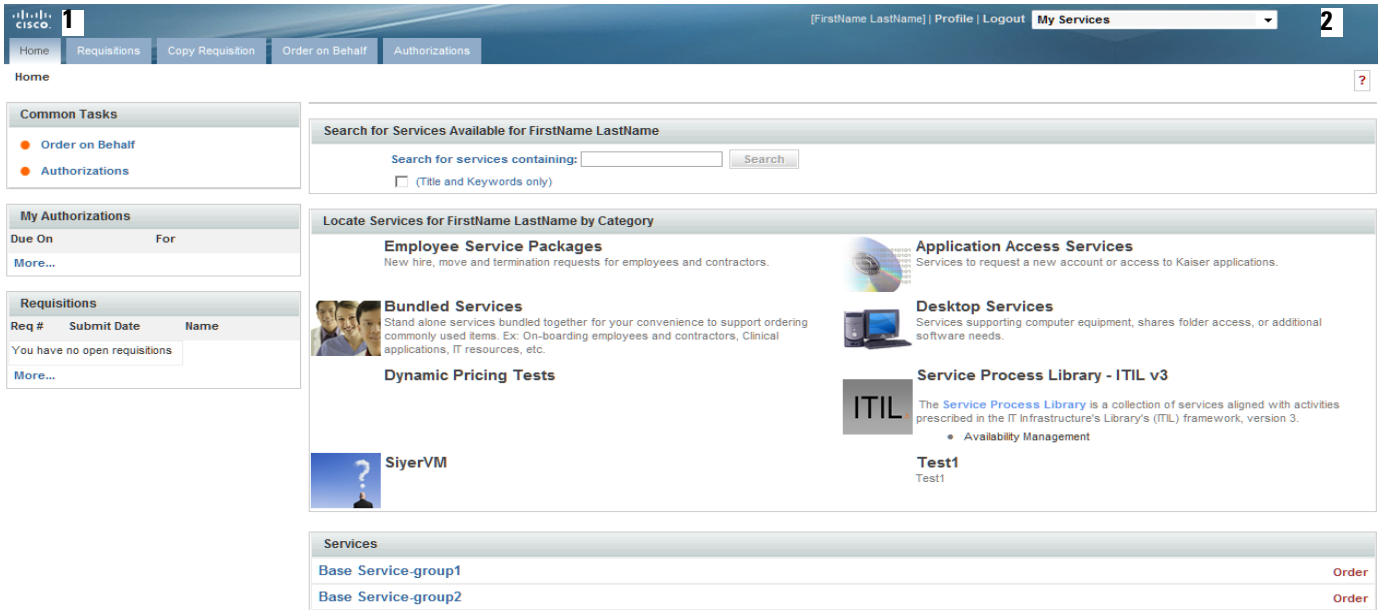
Logo at the right-hand corner (default setting):



1	#leftheaderlogo{
	background: none;
	}

2	#headerlogo{
	background:
	url(/RequestCenter/images/logo_shaded.png)
	top right no-repeat;
	margin-right: 5px;
	min-height:25px !important;
	}

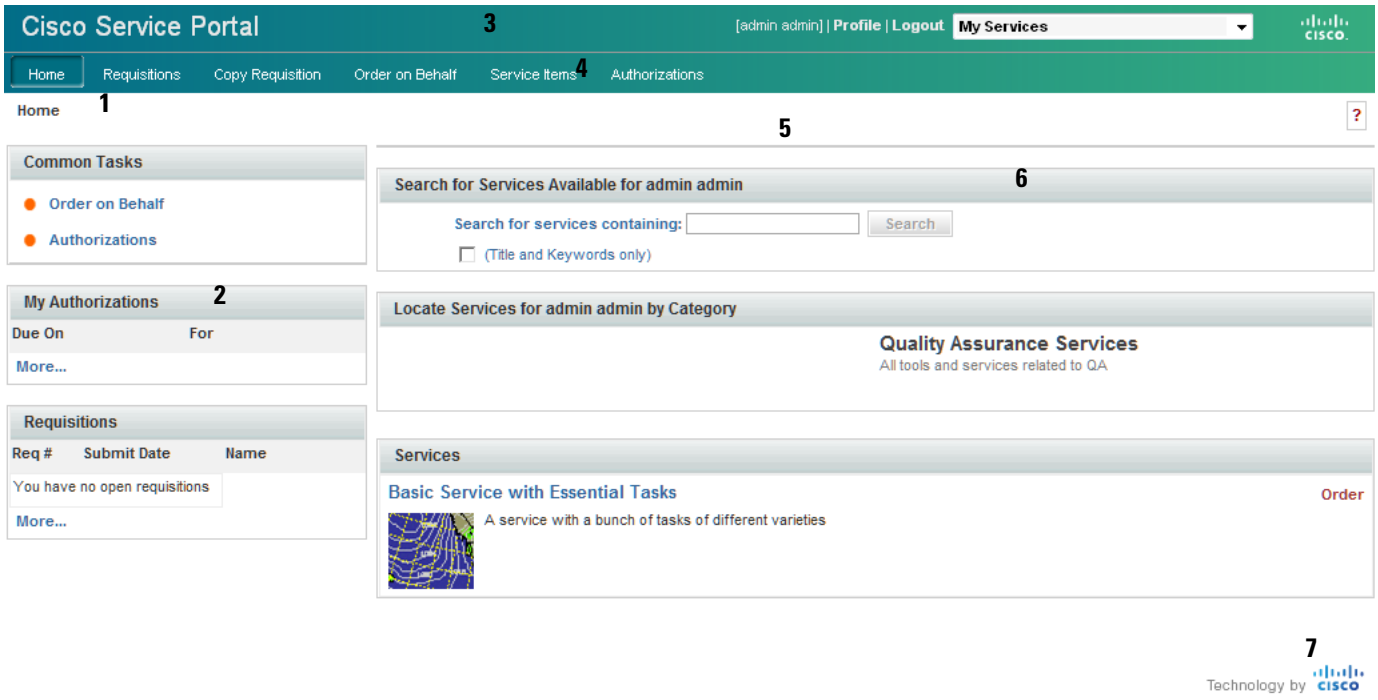
Logo at the left-hand corner:



1	#leftheaderlogo{
	background:
	url(/RequestCenter/images/logo_shaded.png) top left
	no-repeat;
	width:4.5% !important;
	}
	
	#lvl1_nav_title{
	display:none !important;
	}

2	#headerlogo{
	background: none top left no-repeat !important;
	}

Navigation Bars



1	#bread_nav	**5**	#lvl3_nav
2	table.halfGrid	**6**	div.longHeader
3	#lvl1_nav	**7**	#footer
4	.levelTwoNavigation		

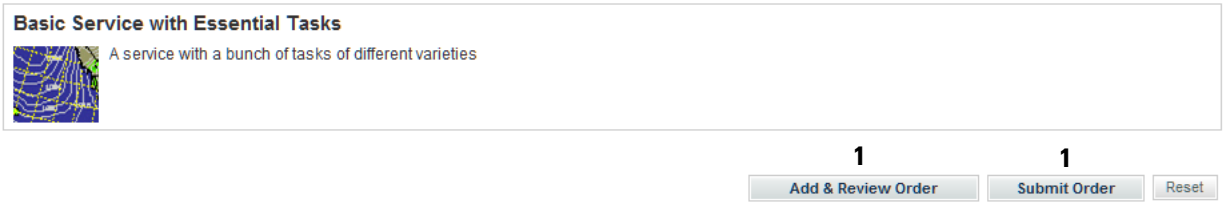
By default, most of the navigation bars simply specify a background color. However, as with any other background designated in the style sheet, this can be changed to use a banner or graphic.

Other portions of My Services and My Services Executive pages use decorations as headers and footers for portions of the page. For example, the “Level3 Navigation” (lvl3_nav) and footer styles delimit the page body of the My Services home page, as shown in the illustration above. They should be changed together.

The “Breadcrumb Navigation” (bread_nav) provides the background for the breadcrumb area.

Buttons

Buttons appear on service forms and through the Service Portal user interface. The appearance of buttons is governed via the style button.primary. The default style for primary buttons is set to use bold face and can be modified to have more prominent styles if necessary.

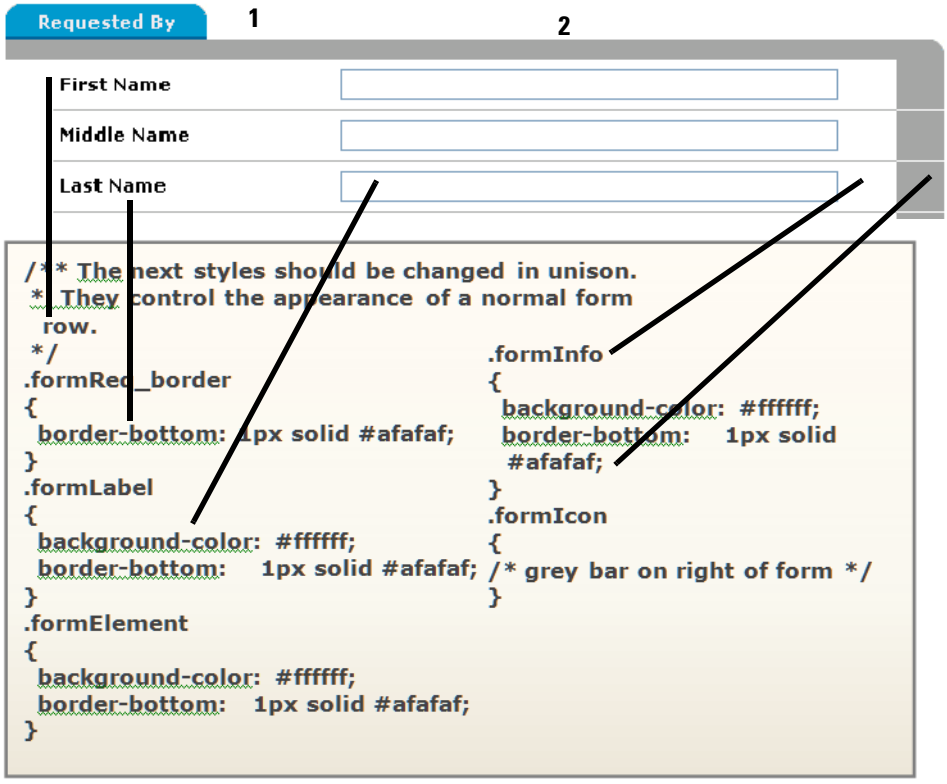


1	Primary buttons

Service Forms

The appearance of the fields and captions displayed on service forms is governed by a set of styles, as shown below and summarized in the following table. All .form styles should be changed in unison.

Style	Usage
shortHeader	The dictionary caption
subhead	The bar delineating the start of each dictionary displayed with a caption
.formReq_border	Blank space to the left of the field label, and the line separating one field from the next
.formLabel	The field label
.formElement	Formatting for the input element for the field's HTML representation
.formInfo	Blank space to the right of the form element, and the line separating one field from the next
.formIcon	Grey bar on the right of the form



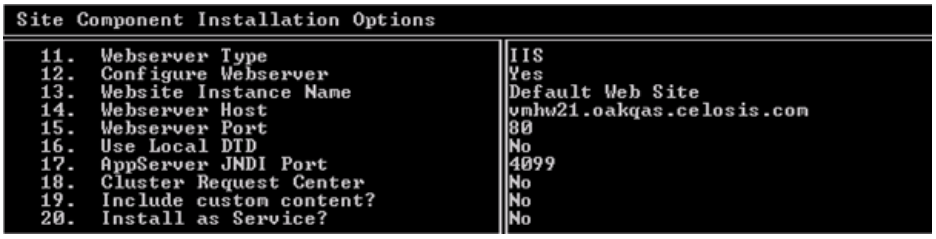
1	shortHeader
2	subhead

Preserving Customizations

The custom style sheet file, as well as html files for defining custom page headers and footers, must be part of the application on the application server. Therefore, a mechanism is required for preserving these customizations in that event that an application instance must be upgraded or migrated. Customizations may be preserved by following the procedure below.

Step 1 Create an archive file (zip or archive type appropriate to the application server platform) containing the files you have customized. The root directory of the archive file should be the RequestCenter.war directory.

Step 2 Perform an upgrade of the Service Portal application. The installation questions pertaining to “Site Component Installation Options” are shown below.



Step 3 Change the response for the question "Include custom content?" (number 19 in this example) to **Yes**. The page display will change, to include an additional question asking you to specify the location of the archive file containing the custom content, as shown below:

Step 4 Enter the directory and name of the archive file.

Step 5 Complete the installation/upgrade process following instructions in the *Cisco Service Portal Installation Guide*. The custom content will be included in the application server deployment package.

Known Errors and Omissions

The on-line help files provided for Service Portal cannot be customized.

Unknown Errors and Omissions

It is possible that some styles used in Service Portal pages are not included in the CustomExamples/example.css file. If you find such an omission, please report it to the Cisco Technical Assistance Center (TAC).

A temporary workaround may be possible. View the source for the generated page, noting the class and/or id of the sections to which the style is to be applied. If this class or id uniquely identified the object whose appearance you want to change, include an appropriate style in your custom stylesheet, or add an appropriate attribute to the style definition. Care should be taken if you elect to use this approach, as any additions to the custom stylesheet may not be supported in subsequent releases.

Upgrading from Previous Versions

The styles used in this version of Service Portal may have been modified from those used in previous versions. These changes not only update the appearance of the pages but also address performance and consistency issues that had been raised in previous releases.

Style Summary and Recommended Practices

Style Summary – Built-in Modules

The table below summarizes styles available in the custom.css.

Style/Class Name	Comment
Body and Global Styles	
body	
#lvl3_nav	
#headerlogo	Right-hand logo
#leftheaderlogo	Left-hand logo
#lvl1_nav_title	Application name
#footer	
.levelTwoNavigation	Tab selection
table#nsLayout.rightMenu td#layoutright	
Navigation Styles	
#lvl1_nav	
#lvl1_nav span #lvl1_nav a	
#llvl1_nav a:hover	
.menuDivider	
#lvl2_nav	
#lvl2_nav a	
#lvl2_nav td.active	
h2#title_nav	
#bread_nav	
#bread_nav a	
#logobottom	Deprecated (dummy image used)
Tab Navigation Control Styles	
.levelTwoNavigation a .tabNavigation a	
.levelTwoNavigation a:hover .tabNavigation a:hover	
.levelTwoNavigation a.selected .tabNavigation a.selected	
.levelTwoNavigation a.selected:hover .tabNavigation a.selected:hover	
.propertyTabNavigation a	
#levelTwoTabDiv img	left and right-edge images on tab button

.levelTwoNavigation div.levelTwoTab	
.levelTwoNavigation a	
My Services Service Items Tab Styles	
.x-grid3-row	background-color for grid row
.x-grid3-row TD	font for grid row
.x-grid3-row-alt	background color for alternate row
.x-grid3-hd-row td	font for grid header
ul.x-tab-strip-top	background color for tabs
.x-tree-node A SPAN	font for tree
Header and Title Styles	
div.longHeader div.shortHeader	
div.longHeader h4 div.shortHeader h4 div.longHeader span div.shortHeader span	
div.subHeader	
h4.header	
h4.header span	
Button Styles	
button input.primary input.secondary input.disabled	
button.primary input.primary	
button.secondary button.help input.secondary	
button.disabled input.disabled	
Catalog and Service Display Styles	
table.browser	
table.browser td.categoryImage table.browser td.categoryText	
table.browser td.categoryText	
div.smallshell	
div.service	
table#columns select	
Data Table Styles	
table. halfGrid,fullGrid,footGrid,taskGrid,noGrid	

table. halfGrid,taskGrid,noGrid	
table. footGrid,noGrid	
table.dProcess	
table. halfGrid,fullGrid,footGrid, taskGrid,noGrid,dProcess thead th.first	
table. halfGrid,fullGrid,footGrid, taskGrid,noGrid,dProcess thead th.firstSel	
table. halfGrid,taskGrid,fullGrid tbody td tbody th	
table. footGrid,fullGrid tbody td tbody th	
table.kpi	
table.fullGrid tbody.subHeader td	
table. halfGrid,fullGrid,footGrid, taskGrid,noGrid,smGrid tbody tr.shade td tbody tr.shade th taskGrid tbody tr.current th tbody tr.current td	
table. halfGrid,footGrid,taskGrid,noGrid tbody tr:hover th td	
table. halfGrid,fullGrid,footGrid, taskGrid,noGrid,dProcess,smGrid thead th body.calendar table#calendar th	
table. halfGrid,fullGrid,footGrid,noGrid tfoot th tfoot td	

table. halfGrid,fullGrid,footGrid,noGrid tbody tr td.select tbody tr th.select	
table. halfGrid,fullGrid,footGrid,noGrid tbody tr td.select + td td.select + th th.select + td th.select + th	
table.fullGrid tbody.td.kvpKeyHi:hover table.fullGrid tbody.th.kvpKeyHi:hover table.fullGrid tbody.td.kvpKeyHi:hover + td.kvpValue table.fullGrid tbody.th.kvpKeyHi:hover + td.kvpValue	
table.fullGrid tbody.td.kvpKeyHi table.fullGrid tbody.th.kvpKeyHi	
table.fullGrid tbody td.kvpValueHi	
Other Tables and Table-Related Content Styles	
div.thead div tfoot	
div.tsubfoot	
div.detailHeader	
div.detailHeader td.owi	
div.tfoot input.textBox div.tsubfoot input.textBox	
Comments and History Styles	
table.commentstable	
table.commentsTable div.commentContainer	
Common Tasks and Portlet Styles	
div.shell	
.commonTaskCell ul.tasks.li	
ul.tasks	
img.commontaskbullet	
Normal Portlet, Form and Container Styles	

div.service div.shell div.smallshell div smallShell table.halfGrid table.fullGrid table.footGrid table.taskGrid table.noGrid #treecontainer div.loginBox	
Input Elements	
input select	Service form text elements
input.textBox textarea	Service form textarea elements
Content-Switching Styles	
ul.MDITabs li:hover	
ul.MDITabs li.active	
Service Form Styles	
tr.error td. formReq formLabel formElement formFlex formInfo	Components of the fields defined in dictionaries used in service forms—the required symbol, the field label, the input element
tr.error td.formIcon	
.formReq_border	
.formLabel	
.formElement	
.formFlex	
.formInfo	
.formIcon	
div#formMonitor div a	
div#formMonitor div.valid	
div#formMonitor div.invalid	
Calendar Styles	
body.calendar table#calendar td	
body.calendar table#calendar td.selected	
Service Manager Styles	
table#SMLayout	
table#SMLayout td#SMTreeFrame	
div.SMToolbar	

table.smGrid tbody tr.hilight td, th	
div. treeHeader treeNode treeItem treeNode span.unselected	
div.treeNode span.selected	
div.treeHeader span	
table.smGrid thead th	
table.smGrid tbody td, th	
table.smGrid tbody tr.shade td, th	
Module Menus	
.modulemenu	
.modulemenu .menuheadingrow	
menuHighlight	

Style Summary – User-defined Modules

The table below summarizes styles available in the portal-custom-header.css.

Style/Class Name	Comment
Header Styles	
#headerlogo	Right-hand logo
#leftheaderlogo	Left-hand logo
#lvl1_nav_title	Application name
#header	
#usercontrols	
#cornerpiece	
#moduleMenuDiv	
.modulemenu	
.menuHighlight	
#userinfoandcontrols	
#userinforow	
#usercontrolstable	
#userconrolsrow	
#profilef	
#logoutref	
#helpref	

Recommended Practices

After cloning from the example.css to create the initial custom.css, the styles should have no effect on the user interface, and as the individual properties are changed, they should then be evident in the customizable modules.

Some styles used by the default user interface are implemented as background images, rather than color values. Some of these images are duplicated in the custom/CustomExamples/images subdirectory, ready for replacement. They should be replaced with images of the same type, size, shape and name in order to be correctly included in the user interface.

There are a number of places in the custom stylesheet where there is an alternative between using a background image and simply specifying a color value. In each of these places, there are alternate attributes that can be commented in or out to determine which of these is to be used. For example:

```
div.longHeader,
div.shortHeader
{   /* background: #FD2312; */
    background: url(./images/headerGradient.gif);
    border-bottom:    2px solid #cc3333;
}
```

Here, the image providing a shaded header for the portlets is being used. To change that gradient, replace this image in the custom subdirectory. To switch to a simple solid background color, comment out the background that specifies the image using the /* */ pattern, and remove the comment from the background with the hex color.

You can also create new images and modify the custom.css file to point to them. For example:

```
#header
{
    background:#ffffff url(./images/logo.gif) top left no-repeat;
    border-bottom: 1px solid #a7a7a7;
}
```

In this case, a new “logo.gif” could be created and the file replaced, or a completely new image generated such as “acme_logo.gif”. Then, the property declaration could be changed to read

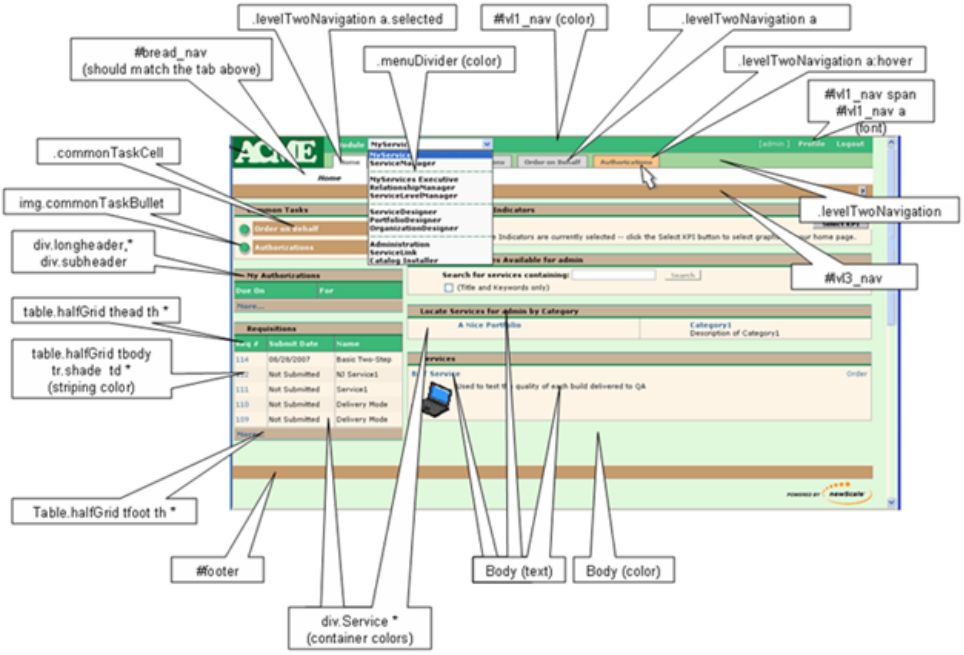
```
    background:#ffffff url(./images/acelogo.gif) top left no-repeat;
```

The same goes for any other image used in the look and feel.

For modules defined and maintained in Portal Designer, the portal page body is not affected by the custom stylesheets. Instead the portal page theme can be configured using “Page Settings” to match with the header styles.

Example Screenshot, and What Each Style Specifically Affects

This diagram is representative of the effect that the styles have. Although it doesn’t include all styles, it does cover the most commonly customized ones.



* Indicates that this is the first descriptor in the style grouping, and there are others.

Custom Headers and Footers

Overview

Cisco supplies a template for customizing the page headers and footers displayed with Service Portal web pages.

Procedure

The procedure below gives the basic steps to follow in order to add a custom header and/or footer to the Service Portal application. Additional details on these styles are given in the following section.

Step 1 Obtain a copy of the files example_header.html and example_footer.html from the custom directory of the Service Portal web archive (RequestCenter.war).

Step 2 Name the copied files as header.html and footer.html, respectively.

Step 3 Add content to the header and/or footer files according to the guidelines given in the next section of this document.

Step 4 Place your custom header and footer files on the specified directory for the style(s) to which they apply. Both files must be present. If you are not using a custom header and/or footer, copy an empty file with the appropriate name and the .html extension to the application server.

Step 5 Use the **Site Administration > Site Configuration** page in Administration to turn on custom headers and footers, by setting the “Enable Custom Header Footer” site configuration parameter to **On**.

Step 6 Restart the browser session of Service Portal—the pages should be displayed with your customizations.

Customizing Page Headers and Footers

Custom page headers and footers are displayed in addition to, not instead of, the standard a page headers and footers. The header and footer html files may contain any html commands deemed appropriate, including use of default Service Portal styles.

For example, using a footer.html file with the following contents:

```
<img src="/RequestCenter/images/eAdmin.gif"
     alt="eAdmin logo" align="top" name="eAdminLogo"/>
```

would result in a footer display like that shown below, where the “Technology by Cisco” logo is the standard page footer in My Services.

CHAPTER 5

System Administration

- Overview, page 5-1
- Startup and Shutdown Procedures, page 5-2
- Ongoing Infrastructure Maintenance Tasks, page 5-3
- Managing the Application, page 5-10
- Performing Application Housekeeping, page 5-24
- Manage Integrations, page 5-30
- Including Custom Content during Installation, page 5-34
- Installing Additional Service Link Adapters, page 5-38
- Configuring SSL for Service Link Inbound Documents, page 5-39
- Configuring SSL for Service Link Outbound Documents, page 5-58
- Troubleshooting , page 5-66
- Errors, page 5-72

Overview

The System Administration chapter addresses the following topics:

- Startup and shutdown procedures for application components
- Recommended backup practices
- Configuration management and customizations of application components
- Ongoing maintenance tasks
- Critical error conditions, error messages, and resolutions

Intended Audience

This chapter is intended for system administrators and other IT professionals who are responsible for supporting Cisco Service Portal (Service Portal). This chapter assumes that you are familiar with enterprise system administration.

Terminology

The designation <APP_HOME> indicates the root directory where Service Portal is installed.

Startup and Shutdown Procedures

This section provides startup and shutdown instructions for the application server, which includes:

- Request Center (including Demand Center, Lifecycle Center, and Portal Manager)
- Request Center Integration Server (Service Link)
- Advanced Reporting Server

JBoss

For a typical installation using the JBoss application server, Request Center is started and stopped along with the application server.

Windows Services

Stop and restart the Request Center and Service Link services.

Command-Line Scripts

A set of commands is installed in the <APP_HOME>/bin directory to allow you to start and stop Request Center services or to install or de-install those services.

Command	Usage
installRequestCenterService.cmd	Install the Request Center service which starts Service Portal.
installServiceLinkService.cmd	Install the Service Link service.
startRequestCenter.cmd	Start the Request Center service as a client process rather than running it as a service.
startServiceLink.cmd	Start the Service Link service as a client process rather than running it as a service.
stopRequestCenter.cmd	Stop the Request Center process.
stopServiceLink.cmd	Stop the Service Link process.
uninstallRequestCenterService.cmd	Uninstall the Request Center service.
uninstallServiceLinkService.cmd	Uninstall the Service Link service.
setEnv.cmd	Script used by commands to install services to set the Service Portal environment.

WebSphere

More detailed information about starting WebSphere can be found in the *Cisco Service Portal Installation Guide*.

When deployed in a network cluster configuration, the node manager may need to be restarted. If it is not possible to restart the server, it is often enough to restart the following applications: Request Center and Service Link using the WebSphere Administration Console.

WebLogic

More detailed information about starting WebLogic can be found in the *Cisco Service Portal Installation Guide*.

The admin server should not need to be restarted during regular Service Portal operation. There is, however, a need to restart it while installing the custom database driver during installation.

Restarting Cognos Server

The instructions for restarting Cognos applications from the Cognos Configuration Manager or using Windows Services are both Windows-specific tasks, as all Advanced Reporting installations that rely on Cognos components are on Windows systems.

Restarting using Cognos Configuration Manager

To restart your system, launch Cognos Configuration Manager and then follow these steps:

Step 1 Select **Program Files > Cognos Tools > Configuration Manager**.

Step 2 Click the **Star Tab > Open Current Configuration**.

Step 3 Select the Machine name (top node in the tree) and right-click to choose **Stop/Start**.

Restarting using Windows Services

Stop the following service and then restart:

- Cognos Business Intelligence (BI) Server – required for all reporting options

Ongoing Infrastructure Maintenance Tasks

This section describes how to perform ongoing maintenance tasks.

Backup Methodology

The components of a fully deployed system include Request Center, Integration Server (Service Link), and Advanced Reporting (Cognos). Request Center and Integration Server are deployed to the application server in the Request Center.ear and ISEE.war deployment packages, respectively.

We recommend backing up each component as it is deployed, and saving any customizations as they are developed or modified. (See the"Installing Additional Service Link Adapters" section on page 5-38 for more information).

Regularly scheduled backups of the databases are also recommended. Three databases need to be backed up:

- The transactional database (by default, Request Center) contains not only production data but also metadata for configuring services, service components, and other application objects.
- The analytical database contains data for building the standard reports, as well as the Request Center and Demand Center data marts.
- The "Content Store" database contains user-generated content available in the business view of the reporting environment. Such content includes the definitions of all reports, both those provided by Service Portal and those written by Advanced Reporting users, as well as report views, schedules, and saved reports generated from any reports.

Application Server Tuning

Please consult the documentation specific to your application server for additional tuning suggestions. The ones listed below have been found to be applicable to many Service Portal sites.

Configuring Service Portal Compression

If your organization has a significant number of distant users, it will make sense to turn on GZIP compression (RFC 1952) for HTTP responses, see RFC 2616:

- Section 3.5: Content-coding
- Section 14.3: Accept-Encoding
- Section 14.11: Content-Encoding

GZIP compression will benefit users working over slow or high latency networks. However, GZIP compression will add a slight overhead on both the server and the user's browser.

Follow these instructions to enable GZIP compression:

Step 1 Locate the web.xml under RequestCenter.war/WEB-INF. For example, a typical location is:

```
C:\CiscoServicePortal\jboss-4.2.3.GA
\server\RequestCenter\deploy\RequestCenter.ear\RequestCenter.war\WEB-INF
```

Step 2 Look for the following entry (which is commented out):

```
<!--filter>
<filter-name>CompressingFilter</filter-name>
<filter-class>com.planetj.servlet.filter.compression.CompressingFilter</filter-class>
</filter-->
```

Step 3 Remove the comments, so the entry becomes:

```
<filter>
<filter-name>CompressingFilter</filter-name>
<filter-class>com.planetj.servlet.filter.compression.CompressingFilter</filter-class>
</filter>
```

Step 4 Look for the following entry (which is commented out):

```
<!--filter-mapping id="newscale_gzip_filter_1">
<filter-name>CompressingFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping-->
```

Step 5 Remove the comments, so the entry becomes:

```
<!--filter-mapping id="newscale_gzip_filter_1">
<filter-name>CompressingFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping-->
```

Step 6 Save the file and restart the application server(s).

Java Memory Settings

Java memory settings are specific to the Java Virtual Machine (JVM) used by the application server. Use the commands “java –h” and “java –X” to return a full listing of the options available on your system. Please ensure that you are calling the same JVM that is used by your application server when issuing these commands.

- -ms –mx as appropriate (usually 1GB of memory is reserved for the heap within the JVM).
- -server mode is recommended for Sun JVM.
- A common modification is to increase the garbage collector’s maximum permanent generation size to 128MB with the argument: --XX:MaxPermSize=128m.

The Java memory switches governing the minimum and maximum heap size available to the JVM may need to be tuned if Service Portal encounters “out of memory” errors. For example, on Weblogic the following settings have been successfully applied.

```
MEM_ARGS="-verbose:gc -Xms500m -Xmx1024m -XX:+PrintGCTimeStamps -XX:+PrintGCDetails
-XX:MaxPermSize=128m"
```

Tomcat Maximum Thread Settings

This setting controls the maximum number of request processing threads to be created by the HTTP or AJP connectors, which therefore determines the maximum number of simultaneous requests that can be handled. In the rare case that the default number of threads runs out and results in ISAPI crash, you can modify the maximum threads with the following steps:

- Edit the file named “server.xml” on the <NS_HOME>/jboss-4.2.3.GA/server/RequestCenter/deploy/jboss-web.deployer directory.
- Do a find of the “maxThreads” setting for connector port 8088. Increase the setting by 50 at a time.
- Restart the Request Center application.

Upgrading/Replacing the JDK

You can upgrade the JDK to a later version by following the steps below:

- Edit the script named “setEnv.cmd” on the <APP_HOME>/bin directory to specify the path to the new JDK.
- For customers using the startup scripts, save the revised setEnv.cmd file and then restart the server.
- For customers using the Windows services, stop the windows services, uninstall the window services (using the <APP_HOME>\bin\uninstall*.cmd scripts), and then re-install the window services again (using the <APP_HOME>\bin\install*.cmd scripts).

Database Tuning

Database tuning for Service Portal databases can be summed up in one sentence: “Use the best practices promulgating for tuning your specific database type, Oracle or SQLServer.”

However, we can list a few of the most frequently asked questions regarding how to configure and tune Service Portal databases and the answers to those questions. For more details on these issues, you will need to consult the appropriate database-specific documentation. Many of these FAQs pertain to Oracle which has more opportunities for tuning than does SQLServer.

- For both Oracle and SQLServer, experts recommend installing the database files on a RAID 1+0 (striped + mirrored) disk, rather than on RAID 5, which is the preferred choice for software installation.
- An Oracle database should be configured to use locally managed tablespaces (LMT) and Automatic Segment Space Management (ASSM). These technologies eliminate previous difficulties with improperly specified table or tablespace parameters (PCTUSED, PCTFREE, INITIALEXTENT, NEXTEXTENT).
- Use different databases/instances for the OLTP Service Catalog and OLAP database (standard reports and the Service Portal data marts). In Oracle releases prior to 10g, this was required in order to create tablespaces with different block sizes. Even in 10g and beyond, it is recommended so that configuration parameters can be adjusted to the vastly different activities in OLTP vs. OLAP databases. Oracle DBAs are urged to read Oracle's excellent documentation on Database Administration for Data Warehouses.

Specific Recommendations for Service Portal

- For the OLTP database, create a primary tablespace named REQUESTCENTER. Allow for 10 MB per user, with a minimum size of 500 MB, for the tablespace. Your database administrator should choose an extent management strategy that fits well with your organization’s best practices.
- A very rough estimate of database storage required is 500kb for each requisition completed. This varies greatly with the complexity of the service form, the authorization structure, and the delivery plan.
- Sites with many Service Link tasks will notice significant growth in the database size, attributable to storing Service Link messages. Recent versions of Service Portal have included increasingly effective compression algorithms for these messages, as well as a means to configure message context. Additional details are available in the *Cisco Service Portal Integration Guide*. Database scripts for purging Service Link messages for completed tasks are available as stored procedures in the RequestCenter database and can be executed either as a one-time job or on a recurring basis.

Tuning Oracle

- Gather statistics on the OLTP database (both tables and indexes) on a regular basis. This can be automated via 10g Oracle Enterprise Manager (OEM).
- Perform column-level histogram analysis to further optimize the Request Center Service Manager indexes.
- Gather statistics on the Service Portal data marts after the data marts have been refreshed.
- Review table allocation, tablespace fragmentation, and row chaining.
- Grant access to the SELECT_CATALOG_ROLE for monitoring query performance.
- For Oracle 10g, apply settings similar to the following:

Parameter	Value
perf.__large_pool_size	16777216
*.processes	300
*.pga_aggregate_target	1059145600
*.sga_max_size	716582400 #internally adjusted
*.sga_target	716582400
*.sort_area_size	500000000

Gather Statistics on the Database

Use the DBMS_STATS.GATHER_SCHEMA_STATS command to gather statistics on all tables and indexes in the RequestCenter database. In the example below, "RC User" is the schema owner.

```
execute DBMS_STATS.GATHER_SCHEMA_STATS(ownname=>'RCUser',cascade=>TRUE);
```

Histogram Analysis

The Oracle Database Administration chapter on "Managing Optimizer Statistics" recommends:

- When gathering statistics on a table, DBMS_STATS gathers information about the data distribution of the columns within the table. The most basic information about the data distribution is the maximum value and minimum value of the column. However, this level of statistics may be insufficient for the optimizer's needs if the data within the column is skewed. For skewed data distributions, histograms can also be created as part of the column statistics to describe the data distribution of a given column.
- Histograms are specified using the METHOD_OPT argument of the DBMS_STATS gathering procedures. Oracle Corporation recommends setting the METHOD_OPT to FOR ALL COLUMNS SIZE AUTO. With this setting, Oracle automatically determines which columns require histograms and the number of buckets (size) of each histogram. You can also manually specify which columns should have histograms and the size of each histogram.

The tables for which it is critical to gather histogram-level statistics are:

- TxActivity
- TxProcess
- TxRequisition
- TxRequisitionEntry
- DirPerson
- DirOrganizationalUnit
- UIEntry

A sample DBMS_STATS command for collecting the statistics on each table would like look:

```
BEGIN
  DBMS_STATS.GATHER_TABLE_STATS (OWNNAME => 'RCUser',
      TABNAME => 'TXACTIVITY',
      METHOD_OPT => 'FOR ALL COLUMNS SIZE AUTO');
END;
```

Tuning SQLServer

For SQLServer 2005, enable snapshots with this command:

```
ALTER DATABASE <database name> SET READ_COMMITTED_SNAPSHOT ON
```

A SQLServer DBCC Reindex command is recommended, especially on volatile Service Portal tables. The process should be regularly scheduled, typically weekly, at off hours.

The tables listed below are the most volatile and should be subject to DBCC Reindex.

TxActivity	TxEventTriggerParam	TxPerformerSummary
TxActivityAssignment	TxIncident	TxProcess
TxAttribute	TxInternalOptionList	TxRequisition
TxCheckList	TxInvocation	TxRequisitionEntry
TxChecklistEntry	TxInvocationAttribute	TxRequisitionStep
TxComments	TxJMSMessage	TxRole
TxCondition	TxJoin	TxRule
TxDictionaryHTMLBindings	TxMultivalue	TxSatisfaction
TxDocument	TxObjectDataHTML	TxService
TxEmailSent	TxObjectDictionaries	TxSubscription
TxEventTrigger	TxObjectRelation	TxTimer

Sizing Cognos Database Components

Cognos maintains the definitions of all reports and queries in a database called the ContentStore. The Cognos KnowledgeBase includes entries on sizing and maintaining the ContentStore. Of particular interest are the formulas published for determining the size required for the ContentStore, based on estimated usage statistics.

A spreadsheet incorporating these formulas is available from the Cisco Technical Assistance Center (TAC). A sample is shown below.

Component	# Estimated	Space per Unit (KB)	Total (KB)
Active Users	250		
Concurrent Users executing reports (Temporary disk space requirements)	50	100,000	5,000,000
Saved Reports 1-10 pages (2 per user, 1-Public, 1 – MyFolder)	500	340	170,000
Saved Reports 10-100 pages (9 per user, 4-Public, 5 – MyFolder)	2250	440	990,000
Saved Views 1-100 rows (3 per user – all MyFolders)	750	250	187,500
Saved Views 100-1000 rows (8 per user – all MyFolders)	2000	350	700,000
Folders Public MyFolders (5 per user)	1,250		0
FrameMaker Models (provided by Cisco)			20,000

Empty Content Store	1	3,000	3,000
Active Schedules (50 Day + 125 Weekly)	175	30	5,250
Total			7,075,750

OLTP Database Tables

The transactional database consists of a set of relational tables that use a prefix naming convention. So, what exactly do these prefixes mean? The following table is provided as an aid to DBAs or others who need to maintain or tune a production database. The structure and contents of these tables is proprietary to Cisco, which reserves the right to freely change table names or structures from release to release.

Prefix	Meaning	Usage
BV	Business Value	Demand Center tables; tables are created even if the Demand Center modules are not deployed; The BV prefix is followed by another prefix (Def, Dir, Tx – all listed in this table) which further indicates the nature of the table. However, all Demand Center tables are written to the default tablespace.
Cnf	Configuration	Tables which contain internal configuration information used by Service Portal; typically, these tables are small and their contents static in a production environment.
Co	Portal Content	Tables which contain Portal Manager Content and Page definitions.
Def	Definition	Tables which hold user definitions of user-configurable objects such as service forms, dictionaries, and checklists; table size varies with the size of the implementation, but is relatively stable in a production environment, typically changed only via usage of the Catalog Deployer.
Dir	Directory	Tables containing person and organizational information; table size for most is quite small (skills, projects, functional positions) and stable; those relating to persons vary greatly per organizational size.
JMS	Java Message Service	Internal Usage.
Mdr	Meta-data Repository	Tables containing meta-data for tables with a (user-defined) dynamic schema (for example. service items, standards, and portal).
Si	Service Item	Tables containing data for service items.
St	Standards	Tables containing data for standards.
Tx	Transaction	Tables which contain all transactions. Tables can be quite large and volatile.
Uc	User Content	Tables containing Portal Manager custom content.
UI	User Interface	Tables which define user-specific customizations for the user interface, such as Service Manager views, the default module displayed on login, and Service Link filters.

Xtr	External	Tables used by Service Link to manage external tasks; the definition tables (XtrDef) may be quite small, but the tables containing messages for external tasks are large and quick-growing.
XtrEUI	External End User Integration	Tables used for Directory Integration definitions.

Managing the Application

This section provides information about the following J2EE application components of Service Portal:

- Request Center – This component comprises the heart of the application—all screens that the user sees, all validation, help screens, and APIs in the Request Center, Demand Center, Lifecycle Center and Portal Manager products.
- Service Link (IS or ISEE) – This is the Integration Server, which uses agents and adapters to allow integration with a variety of third-party systems.

In this section you will learn how to deploy the application, about key configuration files, managing WebSphere, WebLogic, and JBoss, and about how to administer ColdFusion. Additionally, there is information about working with data sources and creating "backing tables" for external data dictionaries, about cached data, application security, applying patches, and multicast settings.

The Basics

Deploying the Application

The .ear file for Request Center is deployed into the file system and contains the .war file that is the presentation layer for the Request Center service. The exact location of these files will vary, depending on application server. For example, in a WebSphere implementation these files are generally found under a path that looks like:

/apps/WebSphere/AppServer/profiles/newScale/installedApps/Cell/RequestCenter.ear

The Service Link application is provided as a .war file, ISEE.war (Integration Server Enterprise Edition.) The WebSphere application server automatically "wraps" an .ear around a standalone .war file.

Restarting the Server

Use the Server Console for your application server or command-line scripts as appropriate to restart the server. Make sure to make a script available to the Administrator in the development environment.

Key Configuration Files

The following are important files that you may need to consult for details on your deployment. Unless specifically stated in this guide or instructed by the Cisco Technical Assistance Center (TAC), all properties files and similar configuration files should be considered read-only. After making changes to any of these property files, you must restart the services.

newscale.properties

This file is created by the installer during the install or upgrade process and any time the installer is run. The file produced by the installer is contained in the RequestCenter.ear/config folder. As such, the file will be redeployed any time the ear is redeployed. The Request Center administrator should preserve the data contained in the file, but should *not* simply restore a copy of the file since the installer may have added new information for the new version. Entries in newscale.properties include:

- udk.datasource.jndi – JNDI name for your RC database
- udk.datamart.jndi – JNDI name for your data mart database
- All registered EJBs

be.properties

This file is located in the root of RequestCenter.ear. Entries in be.properties include:

- ObjectCache.Application.URL – URL reference back to Request Center in the emails sent out
- ObjectCache.email.host – SMTP host for relaying mail
- Container.Datasource – JNDI name for the RequestCenter database
- Scheduler.EscalationManagerSchedule – Schedule for evaluating escalations

bejms.properties

This file is also located in the root of RequestCenter.ear. It contains the JMS settings for Request Center internal communications. Please ensure that the queue names match the ones on the application server.

integrationserver.properties

This file is located in the <APP_HOME>/jboss-4.2.3.GA/server/ServiceLink/conf folder in JBoss systems. For WebSphere and WebLogic application servers, this file is located in the ISEE.war/WEB-INF/classes folder. It contains the key properties of the integration server (Service Link).

Managing Logs

Service Portal maintains log files on the application server to track application activities, both expected and unexpected. Logs are managed using a log4j-based framework, an open source (Apache) logging mechanism. By default, logs are configured as “rolling appenders”, with a new log file opened every day. Location of the log files varies according to the application server type, as does the ability to adjust log file contents and configuration.

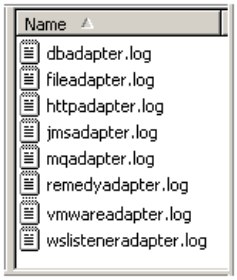
Recommendations:

- Rotate logs on a daily basis (this is the default behavior)
- Keep one month’s worth of logs “online”
- Back up or delete logs that are older than a company-specified retention period

Service Portal does not require log files to be maintained. They are useful primarily as troubleshooting tools in case an error arises.

We recommend against changing the format of the default log files because that’s the format the Cisco Technical Assistance Center (TAC) expects. Rather, customers can create their own appenders that suit their needs.

In addition to the system-wide log files, Service Link is configured to have a separate log file for each adapter type. These logs, too, are managed by log4j. By default, Service Link logging is enabled. The adapter-specific log files, written to the ServiceLink\logs directory, are shown below.



System performance of logging may be an issue. With full DEBUG level enabled, logs get very large very quickly, so logging at full debug and trace levels should be enabled only for short periods. System performance will likely slow down significantly, so logging on a Production system should be kept to a minimum, and only for the length of time required to reproduce an issue.

Sample Log File Entries

There are 4 types of log entries: **E** (Error), **W** (Warning), **I** (Info), **D** (Debug), listed in decreasing order of severity. A sample section of the log might look like the following:

```
[8/22/05 8:58:39:279 CDT]   4643aa LDAPEntryBean E com.newscale.bfw.ldap.LDAPEntryBean
Error matching expression, there might be an open parenthesis in expr
[8/22/05 8:58:39:290 CDT]   4643aa LDAPEntryBean E com.newscale.bfw.ldap.LDAPEntryBean
TRAS0014I: The following exception was logged
org.apache.oro.text.perl.MalformedPerl5PatternException: Invalid option: N
        at org.apache.oro.text.perl.Perl5Util.substitute
        at org.apache.oro.text.perl.Perl5Util.substitute
        at com.newscale.bfw.ldap.LDAPEntryBean.processExpression(LDAPEntryBean.java:328)
at com.newscale.bfw.ldap.LDAPEntryBean.getRegexpAttrValue(LDAPEntryBean.java:296)
[9/11/05 15:01:10:217 EST] 4715bea8 MessagequeueC W
com.celosis.logger.MessagequeueChannel  TRAS0014I: The following exception was logged
java.sql.SQLException: [newScale][Oracle JDBC Driver]There is no process to read data
written to a pipe.
[9/11/05 10:26:22:934 EST] 76b9beb7 UdKernelUtil  W
com.newscale.bfw.udkernel.util.UdKernelUtil  The Cubic's value is NULL
[9/11/05 10:26:22:944 EST] 76b9beb7 OrgUnitDataso I
com.newscale.comps.orgunit.dao.OrgUnitDatasource  Searching Organizational units for
cleaned pattern <%> for PersonID <298 >
```

WebSphere Logging

Request Center routes most messages to STDOUT which WebSphere logs to the SystemOut.log. The SystemErr.log contains any WebSphere errors and information about Request Center timing and memory usage. Both logs can usually be found at a path like:

/apps/WebSphere/AppServer/profiles/cisco/logs/server1

You can enable traces to focus in on a specific area of the application. The trace log for the server can be enabled on a particular Java class or package. General logging and tracing is enabled on any of the exposed classes that appear in WebSphere. Other non-exposed classes can be added as well (although the specific class names would need to be provided by the Cisco Technical Assistance Center (TAC) on a case by case basis depending on the situation under which the logging is required).

Runtime logging is an option which can be chosen through the WebSphere admin console GUI. Runtime logging allows logging and tracing to be enabled for the selected classes without restarting or rebooting the servers or applications.

All log files and locations are typically defined in the log4j.xml file. However, WebSphere has additional control over this as well. For almost any logging in WebSphere, the SystemOut.log file and any other log files in the directory it is located may be referred to and required for troubleshooting. In some cases, there may be adapter log files as well. These will typically be generated wherever the SystemOut.log file is generated for the Service Link server (if running on a cluster). Each node in a cluster will have its own SystemOut.log and related log files, so they may be needed for troubleshooting as required.

The log file properties with respect to trace parameters and locations are controlled by settings in the WebSphere admin console, and / or the log4j.xml associated with the WebSphere server. Enabling logging is fairly intuitive, and is something the WebSphere admin can do.

WebLogic Logging

In WebLogic, Request Center routes messages according to the WebLogic logging configuration. By default, all logging goes to the WebLogic server log, which is usually found in a path similar to the following:

/apps/bea/user_projects/domains/cisco/servers/nsServer/logs/nsServer.log

The default log level is set to INFO, and is adjustable via the WLS Console.

JBoss Logging

The JBoss logs are located under <APP_HOME>/jboss-4.2.3.GA/server/RequestCenter/log/. The jboss-log4j.xml file that determines logging behavior is located under <APP_HOME>/jboss-4.2.3.GA/server/RequestCenter/conf.

Request Center routes most messages to STDOUT which JBoss logs to jboss_out.log. The JBoss_err.log contains any JBoss errors and information about Request Center timing and memory usage.

Improve Logging Performance

To improve performance, modify the jboss-log4j.xml file by adding:

```
<category name="com.newscale">
  <priority value="INFO" />
</category>
<category name="com.celosis">
  <priority value="INFO" />
</category>
```

This modification catches the debug call earlier and eliminates many context switches within the J2EE container.

Administering ColdFusion

Catalog Deployer and service import/export rely on ColdFusion MX 6.1 pages, which are interpreted by a ColdFusion application running in the JEE container. The ColdFusion Administrator can be accessed at:

http://<host>:<port>/RequestCenter/CFIDE/Administrator/index.cfm

The default user name is “admin”.

The ColdFusion Administrator is used primarily to add and delete data sources used by Catalog Deployer.

Adding/Maintaining ColdFusion Data Sources

By default, Service Portal installs and uses the ColdFusion “Request Center” data sources. In addition, Catalog Deployer uses ColdFusion Data Sources to access deployment sites. Such data sources must be created by deployment managers to enable site-to-site transmission of deployment packages.

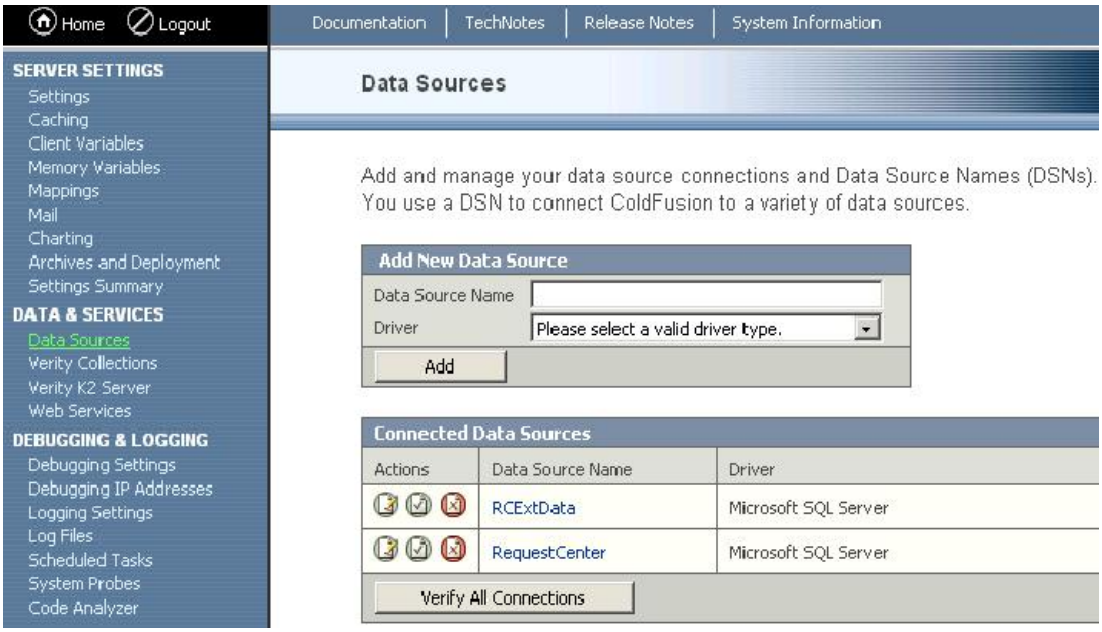
All data sources are case-sensitive within the application.

You use the Cold Fusion Administrator to create a ColdFusion data source. Detailed instructions are given in the *Cisco Service Portal Installation Guide*. In summary:

Step 1 Connect to the ColdFusion Administration URL: http://<hostname>:<port>/RequestCenter/CFIDE/Administrator/index.cfm.

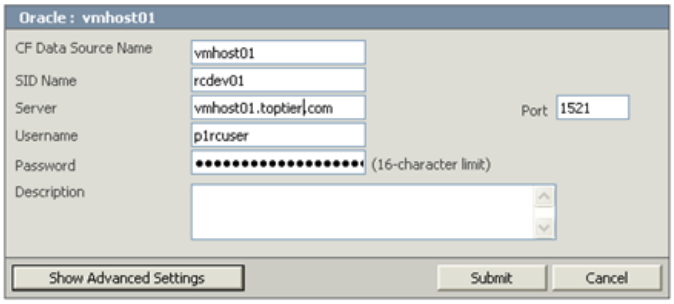
Step 2 Log in with the password = “**A$ta1aV1$ta**”.

Step 3 Click the **Data Sources** link on left panel.



Step 4 To modify or review an existing datasource, click the Data Source Name on the right panel. To create a new data source, enter the data source name, select the driver type and click **Add**. The Data Source Name must correspond to the site name specified in the Administration Entity Homes screen.

Step 5 Enter values for the server, port, database name or SID, username and password.



Step 6 Click **Submit**.

Step 7 Verify the ColdFusion Data source connectivity by using the **Verify All Connections** button.

Data Sources

All modules depend on J2EE data sources, defined via JNDI (Java Naming and Directory Interface). These data sources must point to the correct database and have the appropriate login information configured. For JBoss, the JNDI data sources reside in the <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy directory.

Request Center Core Data Sources

The installer automatically creates two data sources:

- The transactional data source. This will be named requestcenter-ds.xml for installations created with versions 2008.x and greater. For installations upgraded from previous versions, the data source name will reflect the underlying database: oracle-ds.xml or mssql-ds.xml.
- The data source for the reporting database, including the data marts, named datamart-ds.xml.

Additional Data Sources

Additional JNDI data sources are required if:

- External dictionaries are used.
- Customer-specific data sources are accessed by data retrieval rules or by option lists in a service definition that are based on a SQL statement or a relational database table.

Accessing external data sources on a type of database different than Service Portal (for example, a SQLServer data source accessed from an instance of Service Portal running on Oracle, or a Sybase data source accessed from any instance of Service Portal) is not supported in a service form.

Procedures for configuring data sources are detailed in the *Cisco Service Portal Installation Guide*, and are specific to the application server.

Adding Data Sources

All data sources to be accessed by data retrieval rules or option lists must have corresponding JNDI data sources. Add new data sources that contain data accessed by the Request Center module to the J2EE Application Server Data Sources.

When you add data sources, you should use the Cisco drivers if possible.

JBoss

Additional datasource definitions must reside in the <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy directory. The easiest way to create a new data source is to copy the XML file for the Request Center data source and change the JNDI name and connection criteria as appropriate.

The datasource definition for SQLServer databases typically requires the server name and port number. This approach, however, does not work for named instances with dynamic port numbers. To access such instances, specify the database name\instance name, and omit the port number.

Websphere

- Use the JDBC Provider on WebSphere. Support for the RAR deployment has been deprecated for stability reasons.
- Restart the Node and Node Manager after adding the provider or making any modifications to the data sources.

Creating "Backing Tables" for External Dictionaries

External dictionaries within Request Center need to be "backed" by physical tables in the database. You cannot have read-only external dictionaries. All external dictionaries are read-write. Only Request Center should write to External Dictionaries.

For Request Center to relate External Dictionaries to the Requisition, a numeric column needs to be available that can be used as the foreign key. This is typically named RequisitionEntryID.

Sample SQL Listing to Create a Backing Table

This code creates a sequence that generates unique ids for each row. Creating an index on the RequisitionEntryID column greatly optimizes Service Manager performance.

The backing tables for external dictionaries are not transported by Catalog Deployer across environments. Only the dictionary definition can be deployed, as a component of a service.

```
create sequence X_SEQ;
create table (
  X_ID INT CONSTRAINT PK_X primary key,
  REQUISITION_ENTRY_ID INT,
  REQUESTORLANID VARCHAR2 (10),
  REQUESTORNAME VARCHAR2 (50),
  FUNDINGSOURCECODE VARCHAR2 (15),
  DATENEEDED DATE,
  REASONFORCHANGE VARCHAR2 (50),
  PROJECTNAME VARCHAR2 (50),
  TOPINITIATIVE VARCHAR2 (5));

create or replace trigger X_it
```

```
  before insert on X for each row
declare
  seq_val number;
begin
  select X_seq.nextval into seq_val from dual;
  :new.X_ID := seq_val;
end;
```

Applying Maintenance Releases and Patches

Detailed information about applying a maintenance release can be found in the Release Notes that accompany the release, or the readme file in the case of patches.

Some patches may simply require you to add or replace content in the currently installed deployment environment. In this case, the instructions in the readme would list, step by step, the procedures to follow and what software needs to be replaced.

Maintenance release and certain patches may require a complete upgrade/re-install of the Service Portal deployed environment. In this case, please ensure that you preserve any customizations and reapply them after the upgrade/re-install.

Configuring Service Export via SSL or NTLM

The Service Export feature in Service Designer establishes a connection to Request Center, retrieves the exported XML, stores it in a file, and returns a link to the user.

If the application is SSL-enabled, then the user will encounter a problem when trying to export a service as an XML document. The connection to Request Center needs to authenticate to the server, and Request Center needs an SSL certificate. Follow the instructions below to enable the “export service” feature when Request Center is SSL-enabled.

Step 1 Export the trusted root CA certificate used by the Request Center web server, in Base 64 Encoding format, into a file. The file will most likely have an “.arm” or “.cert” extension. This is a simple text file that can be opened in any text editor.

Step 2 Find the CA certs keystore that comes with the Java installation on your Request Center machine. The CA certs keystore for your Java installation is a file named cacerts.

- For JBoss, cacerts is located in <JAVA_HOME>\jre\lib\security.
- For WebSphere, cacerts is located in <WAS_HOME>/java/jre/lib/security.

Step 3 Import the trusted root CA certificate of the Request Center web server into the Java’s cacerts keystore. You can use either the Java keytool utility, or the IBM ikeyman utility if you are on a WebSphere environment.

- The keytool.exe program can be found in the <JAVA_HOME>/bin directory. For WebSphere, the Java keytool.exe program is located in the <WAS_HOME>/java/jre/bin directory.

  The following example provides the command line syntax for the Java keytool utility, which will import the root CA certificate into cacerts:

  ```
  keytool.exe -import -trustcacerts -alias RC
  -file <root_cert_file>
  -keystore C:\jdk1.6.0_12\jre\lib\security\cacerts
  ```

  where <root_cert_file> is the full pathname of the file that contains the root CA certificate of the Request Center web server which you exported in step 1.

The keytool program will prompt you for a keystore password. For a new installation of Java, the default keystore password for the "cacerts" file is "changeit". Enter **changeit**, or another value if you have already changed the password since you installed Java on this machine.

If the question "Trust this certificate?" appears, enter "**y**".

Re-start the application server instance, in order for the changes to take effect. Re-start the whole instance (of JBoss, WebSphere or WebLogic n this machine, and not just individual server, or individual application.

Request Center Cached Data

Site Configuration Settings

Most site configuration settings are cached in the J2EE system for faster access. To reload any settings that are used by the J2EE application, change any option on the Settings page of the Administration module and click the **Update** button. This invalidates the cache and reloads the settings from that page.

Business Engine Caching

Request Center includes a proprietary work flow management system, sometimes referred to as the "Business Engine". The actions of the Business Engine—managing the delivery plan—are largely transparent to application users, since they happen "behind the scenes", that is, on the application server. However, a user interface is provided for system administrators to view and possibly adjust Business Engine operation.

Users with the Site Administrator system role can access the Business Engine console via the URL http://<serverName:portNumber>/RequestCenter/businessengine/index.jsp. There you can:

- View the Business Engine configuration
- Delete the Object Cache
- Force a run of the Escalation Manager
- View the transaction cache log

Request Center Data Security

Database Security

User passwords are usually not stored in the database if external authentication via SSO is used. When they are, they are a one-way MD-5 hash. Passwords stored in configuration files or in the database are encrypted using a Public/Private key encryption. No additional encryption is applied to the data.

The **UseStrongEncryption** option available in the Administration module settings controls AES 128-bit encryption of all form data, but some performance degradation may occur. The data is compressed prior to encryption. This setting cannot be changed once it has been enabled. It cannot be used for sites that wish to use the Service Portal data mart, including form data.

Configuration Files

Database passwords in configuration files are encrypted. When Service Link is configured, the J2EE container password is not encrypted and is stored as plain-text in several configuration files.

URLs

URLs are not encoded; data-level security verifies authorization for each screen. URL encoding/encrypting will be enabled in version 2006.1+ and non-encoded URLs will be rejected by the server.

Application Security

Setting up Secure LDAP

- Retrieve SSL certificates from the LDAP server.
- Ensure LDAP server supports SLDAP connectivity (typically on port 636).

Request Center maintains a password-protected key-store that can store many certificates.

SSL

It is recommended that the web server, or the content switch in front of the web server, run SSL, especially in Extranet-supported environments.

Web Server to Application Server communication does not usually need to be encrypted.

Removal of CGI support in Advanced Reporting

Several tools scan applications to ensure that no CGI-based submits (GET Form submissions) exist in the application.

Cross-Site Scripting

Cisco is focused on the security and safety of your data and is well-aware of the threats presented by XSS (Cross-site scripting) attacks.

Request Center uses a standard J2EE **input-filter-config.xml** file to check that URLs do not contain any of the following characters: < > " ' ( ) & ;

This file is located in: RequestCenter.war\WEB-INF\config\.

Reporting and Advanced Reporting

The Reporting and Advanced Reporting modules require scripts that maintain the Request Center and Demand Center data marts and produce the standard reports and KPIs available to users.

Reporting Batch Programs

Service Portal Extract-Transform-Load (ETL) scripts generated from the Cognos DataManager ETL tool control the population of the database which supports running pre-built reports provided by Service Portal and all non-form based data in the data mart.

Additional command files complete the generation of the framework used by Cognos QueryStudio and Report Studio (Ad-Hoc Reports and Report Designer) to permit ad-hoc reporting on the Request Center and Demand Center data marts.

These scripts share the same invocation and logging framework. They are available as Windows .cmd files that reside and run on the Cognos server. They can be scheduled to run via any enterprise scheduler. These scripts log their activities in the newScale\log directory of the Cognos server.

The following script is required to support standard reports and Key Performance Indicators (KPIs).

Program	Description/Usage
update_datamart_std.cmd	Populates database tables which support the pre-built reports according to ETL rules specified in Data Manager. This is a complete rebuild of the database contents, rather than an incremental refresh. Produces a log file in <*cognos.root*>*c8**datamanager*\log.

The following programs are required to support the data marts.

Program	Description/Usage
update_datamart.cmd	Populates the data mart fact and dimension tables using rules specified in Data Manager, as well as the Demand Center data mart. This is an incremental refresh of all static dimensional and fact data. It produces a log file in <*cognos.root*>*c8**datamanager*\log.
create_model.cmd	Creates a Cognos FrameworkManager model that includes dynamically defined reportable objects (dictionaries and services) as well as standard facts and dimensions. The model is rebuilt by merging a statically defined model (the standard facts and dimensions used in the data marts) with dynamically generated metadata describing reportable services and dictionaries.
publish_fdr_pkg.cmd	Publishes the FrameworkManager model to the Cognos BI Server, via the Cognos ScriptPlayer utility. Must be run as part of the Service Portal data mart refresh, following the program that creates the model (create_model.cmd).

Form-Data Extraction Script

Dictionaries and services designated as reportable are populated in the data mart by a Java program. The program's activities are logged in the current log file on the application server.

This program is run via the internal scheduler. Schedule settings can be specified as part of the installation or modified by editing the newscale.properties file. The following properties configure the scheduler. We recommend running the ETL (and other processes) daily. The data mart will not be usable when the job is running. The ETL process is run with transaction logging. It may be advisable to increase the transaction size (FDR_ETL_RECORDS_PER_BATCH).

```
#Enable ETL Process: 0 or 1 (1=Yes, 0=No)
ENABLE_FDR_ETL_PROCESS=0

# FDR_ETL_TRIGGER : 1 for hourly, 2 for daily, 3 for minutes
FDR_ETL_TRIGGER=1

#Frequency Hourly
FDR_ETL_TRIGGER_FREQUENCY_HOURLY=5

#Daily Time HH:MM (22:30 for 10:30 PM)
FDR_ETL_TRIGGER_FREQUENCY_DAILY=22:30

#Frequency in minutes
FDR_ETL_TRIGGER_FREQUENCY_MINUTES=1

#Number of records per batch insertion
FDR_ETL_RECORDS_PER_BATCH=500
```

Escalation Manager

The Escalation Manager is responsible for monitoring if/when a task exceeds its Operating Level Agreement (OLA). If the OLA is exceeded, and escalations have been configured, the Escalation Manager sends the appropriate notifications after the designated amount of time has elapsed since the task became overdue.

The Escalation Manager is run via the internal scheduler. Schedule settings can be adjusted by editing the be.properties file. By default the Escalation Manager is set to run during business hours Monday through Friday.

A schedule setting is essentially a cron expression, which describes the desired schedule in the format “Seconds Minutes Hours Day-of-Month Month Day-of-Week”. For example, the expression “0 0 12 ? * WED” means “every Wednesday at 12:00 pm”.

Service Manager

Service Manager is the module used by task performers and to fulfill service requests.

Service Manager allows users to search for tasks or requisitions of interest by specifying a set of conditions to be matched, via the Filter and Search pop-up window. By default, these conditions do not support a “contains” operator, for example, the ability to find all task whose name contains a specified string.

This default behavior optimizes performance by increasing the probability that indexed queries can be run against the database. The functionality of performing “contains” queries can be supported; however, administrators should be careful in making this configuration change, as response time may not be optimal, especially with a large transactional database. Reverting back and forth is not recommended as it will impact Service Manager’s Custom Views.

To allow Service Manager users to specify “Contains” queries, edit the newscale.properties file, to add the following property setting:

```
# Service Manager will use this flag to control Contains Query in Datatable Filter and
Search

ContainsQueryInFnS=true
```

As with all changes the properties files, the services must be stopped and restarted for this change to take effect.

Relationship Manager

Relationship Manager is the module used for managing a tailored portfolio of Service Offerings for business unit executives. The Relationship Manager Home page can be configured to appear with or without the browsing carousel by editing the newscale.properties file setting:

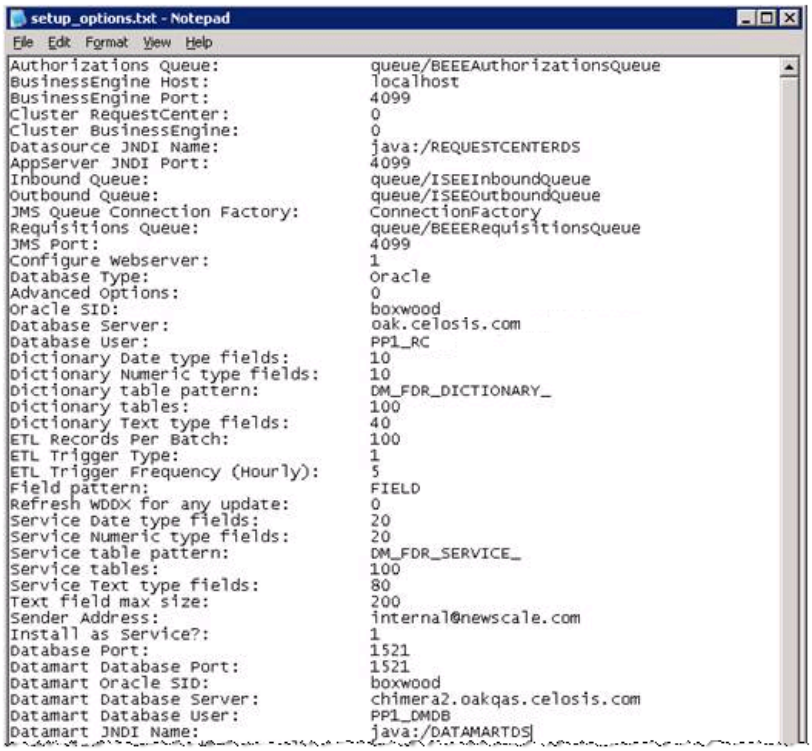
rm.enable.carousel=false

By default the setting is false, meaning that the carousel is disabled.

Service Portal Installation

Installation settings are recorded in the RequestCenter/etc folder. Preserve that folder so that installation settings are “remembered” for future invocations of the Service Portal Installer.

The settings are available in the file setup_options.txt. A sample is shown below.



Each time the Installer is invoked, the logs of actions processed are written to the <APP_HOME>/logs folder with a mmddyyyyhhmm time-stamp (for example, 010720111126). Key installation logs are listed below.

File Name	Contents
RC_Install	General installation logs.
RC_File	Information about any files that were added, moved, or deleted from the file system.
RC_DbInstall	Information about the SQL scripts executed during the database installation/upgrade process, including the time taken for each script to execute.
RC_Sql	Log of the SQL statements that were run on the database during the install. This log may be particularly useful if a SQL script fails during the installation, as the log will contain the text of the script which caused the error and indicate the exact nature of the error.

Multicast Settings

A single clustered installation of Request Center requires multicast to communicate within the cluster. Each node has to be on the same subnet or have multicast routing enabled across the subnets on the switches. You may also have to enable multicasting in the network interface configuration of the host servers.

Request Center uses multiple multicast addresses that have to be unique.

Testing Multicast Connectivity

Test 1 – Can Node1 talk to Node2?

- Choose a valid multicast address and port that are not in use.
- On Node2: java -classpath .:./javagroups-all.jar org.javagroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555.
- On Node1: java -classpath .:./javagroups-all.jar org.javagroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555.
- On Node1 you see a prompt “>”.
- Type in some text and hit [Return].
- Your text appears on Node2.

Test 2 – Can Node2 talk to Node1?

Repeat Test1 with Node2 as the Sender and Node1 as Receiver.

Performing Application Housekeeping

Requistion Purge

Overview

Service Portal provides a transaction purge feature to delete transactions older than a chosen date or that meet other user-specified criteria. This allows the application administrator to remove test requisitions before deleting test users and sample services. The purge scripts may also be used for housekeeping purposes to control the database size, for example, to delete older requisitions that no longer need to be retained. However the purge scripts are not optimized for mass data deletion and should be used with caution to avoid prolonged maintenance window.

Pre-requisite software for the purge utility is a database client on the machine where the purge scripts are to be executed. For Oracle, “sqlplus” has to be installed and configured to connect to the RequestCenter database; for SQL Server, “osql” is required.

Preparations

Step 1 Make a backup of the RequestCenter database before executing the purge scripts.

Step 2 Stop the Request Center and Service Link services while the purge scripts are executed.

Step 3 Locate the utility in:

<APP_HOME>**\schema\util\purge**

Step 4 If the machine where <APP_HOME> resides has the pre-requisite database client software, then you can execute the purge scripts from this machine. Otherwise, copy the entire **purge** folder to the machine where the RequestCenter database is located, or to another machine that has the pre-requisite database client.

Step 5 Verify that the **purge** folder contains the following files:

- AddPurgeFilter.bat
- AddPurgeFilter.sh
- ClearAllPurgeFilter.bat
- ClearAllPurgeFilter.sh
- PurgeRequisitions.bat
- PurgeRequisitions.sh

Step 6 Execute the .bat files if you are on Windows operating system, or the .sh files if you are on UNIX or Linux operating system.

Caution If you have applied any Service Portal service packs, repeat Steps 3 and 4 above, to ensure that you use the latest version of the purge scripts, as the scripts may be modified as part of the service packs.

Using the Scripts

Follow the steps below to define and execute the requisition purge:

Step 1 Clear purge filter criteria.

Step 2 Configure purge filter criteria.

Step 3 Perform a dry run for the requisition purge.

Step 4 Perform the actual requisition purge.

Clearing Purge Filter Criteria

This step is not required if the same filter criteria are always used for purging requisitions (for example, purge all cancelled requisitions). However, as a good practice, it is recommended that the criteria from the previous run are cleared first to avoid confusion.

Use the **ClearAllPurgeFilter** script to clear one or all filter criteria. If [*Purge Filter Name*] is not given, the script will remove all filter entries from the **CnfPurgeFilter** table in the RequestCenter database. Otherwise, the script removes only the specified [*Purge Filter Name*] if it exists in the **CnfPurgeFilter** table.

Oracle:

ClearAllPurgeFilter ORACLE [*SID*] [*User*] [*Password*] [*Purge Filter Name* (optional)]

SQL Server:

ClearAllPurgeFilter SQLSERVER [*Server*] [*Database*] [*User*] [*Password*] [*Purge Filter Name* (optional)]

Possible values for the optional [*Purge Filter Name*] are:

- CREATIONSTARTDATE
- CREATIONENDDATE
- CLOSEDSTARTDATE
- CLOSEDENDDATE
- REQUISITIONSTATUS
- REQUISITIONID
- SERVICEID
- SERVICENAME

Adding Purge Filter Criteria

Use the **AddPurgeFilter** script to add one or more filter criteria. Requisitions will be deleted only if they meet all the purge criteria. The filter criteria are stored in the table **CnfPurgeFilter** in the RequestCenter database.

Use the command syntax below appropriate to your database type:

- [*SID*] is the ORACLE_SID for Oracle database
- [*Server*] is the SQL Server database server name
- [*User*] is “RCUser”

- [*Password*] is the password for "RCUser"
- Refer to the parameters table for possible values for [*Purge Filter Name*] and [*Purge Filter Value*]

Oracle:

AddPurgeFilter ORACLE [*SID*] [*User*] [*Password*] [*Purge Filter Name*] [*Purge Filter Value*]

SQL Server:

AddPurgeFilter SQLSERVER [*Server*] [*Database*] [*User*] [*Password*] [*Purge Filter Name*] [*Purge Filter Value*]

Purge Filter Name	Description	Purge Filter Value
CREATIONSTARTDATE	Purge requisitions created on or after this date.	Date in DD-MON-YYYY format.
CREATIONENDDATE	Purge requisitions created on or before than this date.	Date in DD-MON-YYYY format.
CLOSEDSTARTDATE	Purge requisitions closed on or after this date.	Date in DD-MON-YYYY format.
CLOSEDENDDATE	Purge requisitions closed on or before than this date.	Date in DD-MON-YYYY format.
REQUISITIONSTATUS	Purge requisitions with the specified status.	Possible values are OPEN, CLOSED, CANCELLED or ALL.
REQUISITIONID	Purge a specific requisition based on the Requisition ID.	Unique number assigned to the requisition.
SERVICEID	Purge requisitions that contain a specific service based on the Service ID.	Unique identifier of the service, as displayed on the Service Designer General page for the service definition.
SERVICENAME	Purge requisitions that contain a specific service based on the Service Name. For SERVICEID and SERVICENAME filters, the complete requisition is deleted—including all service requests. Purge is at the requisition-level, not at the individual entry-(service) level.	Service Name enclosed in double quotes, for example, "Email Service". **Note** This purge filter value must be an exact match, and is case-sensitive. **Note** On UNIX or Linux operating systems, do not use this purge filter if the Service Name contains spaces.

Performing a Dry Run for Requisition Purge

Before purging requisitions, you may optionally perform a "dry run" that to see which requisitions would be removed without actually deleting them. This will serve as a validation for the filter criteria in effect.

Use the **PurgeRequisitions** script to get a list of requisitions which meet the filter criteria.

Oracle:

PurgeRequisitions ORACLE [*SID*] [*User*] [*Password*] **PURGE**

SQL Server:

PurgeRequisitions SQLSERVER [*Server*] [*Database*] [*User*] [*Password*] **PURGE**

The list of requisitions found in a dry run is stored in the **LogPurge** table in the RequestCenter database. The log entries are appended to the table with a RunID incremented by 1 for every execution. You can review the requisitions to be purged by querying the LogPurge table entries with the highest RunID.

The **LogPurge** table can grow quickly over time, if you perform many dry runs and requisition purges. Therefore, it is recommended that you manually truncate the **LogPurge** table periodically to remove entries from previous runs.

You can repeat Steps 1 to 3 to revise the purge criteria. Once the purge filter criteria have been finalized, you can proceed with the actual requisition purge.

Performing the Requisition Purge

The requisition purge removes those requisitions that meet the purge filter criteria and all transactional data associated with those requisitions, including tasks and Service Link messages.

Results from the actual requisition purge are also appended to the **LogPurge** table in the RequestCenter database. To perform the actual requisition purge, use the same command **PurgeRequisitions** with the PURGE parameter as shown below.

Oracle:

PurgeRequisitions ORACLE [*SID*] [*User*] [*Password*] **PURGE**

SQL Server:

PurgeRequisitions SQLSERVER [*Server*] [*Database*] [*User*] [*Password*] **PURGE**

Workflow Purge

The workflow purge utility removes temporary data from the database related to workflow processing. Those data are no longer used in the product and can be removed to reduce the database size. Executing the purge utility periodically could also provide overall performance improvement.

The workflow purge utility is provided in the form of a stored procedure in the RequestCenter database. The purge utility can require an hour or more to execute if you have a large database. Hence the purge should be done during system down time or a low activity time window. A practice run is recommended on a sandbox environment to establish how long the script will run for your database.

To track the start/end times for the purge, enable the setting for displaying print statements in the SQL tool before you execute the stored procedure.

Running the Utility on an Oracle Database

To run the utility on an Oracle database:

Step 1 Back up the RequestCenter database.

Step 2 Use a query tool appropriate for your database (for example, SQL*Plus) and connect to RequestCenter database as the RCUser.

Step 3 Execute the following commands:

- SET SERVEROUTPUT ON

- EXECUTE sp_PurgeWorkflowTables;

At the end of the execution, the total elapsed time should be displayed. Here is an example of the output:

```
Creation/Data population of TxReq_temp-    Successful
Time taken for TxReq_Temp   : .17 s
Creation/Data population of TxReqEntry_temp-    Successful
Time taken for TxReqEntry_Temp   : .08 s
Creation/Data population of TxSubscription_Temp -    Successful
Time Taken for TxSubscritpion   : 5.39 s
Creation/Data population of TxProcess_Temp -    Successful
Creation/Data population of TxJoin_Temp -    Successful
Time Taken for TxJoin   : .91 s
Creation/Data population of TxCondition_Temp -    Successful
Time Taken for TxCondition   : 1.18 s
Creation/Data population of TxActivity_Temp -    Successful
Creation/Data population of TxEventTrigger_Temp -    Successful
Creation/Data population of TxEventTriggerParam_Temp -    Successful
Time Taken for TxEventTriggerParam   : .33 s
***Creation/Data population of TxEventTrigger -    Successful***
***Creation/Data population of TxProcess -    Successful***
Creation/Data population of XtrChannelInfo_Temp -    Successful
Creation/Data population of XtrChannelParameterSpec_Temp -    Successful
***Creation/Data population of XtrChannelParameterSpec -    Successful***
Elapsed time: 10.62 s

PL/SQL procedure successfully completed.
```

Running the Utility on an SQL Server Database

To run the utility on an SQL Server database:

Step 1 Back up the RequestCenter database.

Step 2 Use a query tool appropriate for your database (for example SQL Server Management Studio) and connect to RequestCenter database as the RCUser.

Step 3 Execute the following command:

- EXECUTE sp_PurgeWorkflowTables

At the end of the execution, the total elapsed time should be displayed. Here's an example of the output:

```
(2258 row(s) affected)
Creation/Data population of TxReq_Temp-    Successful
Time taken for TxReq_Temp   : 0 s
(2639 row(s) affected)
Creation/Data population of TxReq_Temp-    Successful
Time taken for TxReqEntry_Temp   : 0 s
(56580 row(s) affected)
(0 row(s) affected)
(56580 row(s) affected)
Creation/Data population of TxSubscription_Temp -    Successful
Time taken for TxSubscription_Temp   : 6 s
(4551 row(s) affected)
(2 row(s) affected)
Creation/Data population of TxProcess_Temp -    Successful
Time taken for TxProcess_Temp   : 0 s
(4154 row(s) affected)
(0 row(s) affected)
(4154 row(s) affected)
Creation/Data population of TxJoin_Temp -    Successful
```

```
Time taken for TxJoin_Temp   : 1 s
(9382 row(s) affected)
(9382 row(s) affected)
Creation/Data population of TxCondition_Temp -    Successful
Time taken for TxCondition_Temp   : 2 s
(7017 row(s) affected)
Creation/Data population of TxActivity_Temp -    Successful
Time taken for TxActivity_Temp   : 0 s
(5528 row(s) affected)
Creation/Data population of TxEventTrigger_Temp -    Successful
Time taken for TxEventTrigger_Temp   : 0 s
(1202 row(s) affected)
Creation/Data population of TxEventTriggerParam_Temp -    Successful
Time taken for TxEventTriggerParam_Temp   : 0 s
(5528 row(s) affected)
***Creation/Data population of TxEventTrigger -    Successful***
(1202 row(s) affected)
***Creation/Data population of TxEventTriggerParam -    Successful***
(4553 row(s) affected)
***Creation/Data population of TxProcess -    Successful***
(645 row(s) affected)
Creation/Data population of XtrChannelInfo_Temp -    Successful
Time taken for XtrChannelInfo_Temp   : 0 s
(8409 row(s) affected)
(8409 row(s) affected)
***Creation/Data population of XtrChannelParameterSpec -    Successful***
Elapsed time: 11 s
```

Service Link Messages Purge

The Service Link Message Purge Utility removes nsXML messages from the database. Since these messages can be quite large (depending on the complexity of the service form and content type option used to configure the agent), removing the messages greatly reduces the database size required to hold Service Link-related data. External messages remain unchanged.

Running the Utility on an Oracle Database

To run the utility on an Oracle database:

Step 1 Back up the RequestCenter database.

Step 2 Use a query tool appropriate for your database (for example, SQL*Plus) and connect to the RequestCenter database as the RCUser.

Execute the following commands:

SET SERVEROUTPUT ON

EXECUTE exec sp_CleanupSlMessageContent (<n>);

where <n> = Number of days for which completed/failed Service Link messages are to be retained; -1 means all completed/failed messages will be purged.

At the end of the execution, the total number of messages purged and elapsed time should be displayed. Here is an example of the output:

```
Updating messages with MessageStateID 2 (completed) or 3
(failed) that are older than 100 days
Done updating 3200 messages
Script Start Time 07/06/2011 02:07:11 and script End Time
07/06/2011 02:09:11
```

Running the Utility on an SQL Server Database

To run the utility on an SQL Server database:

Step 1 Back up the RequestCenter database.

Step 2 Use a query tool appropriate for your database (for example, SQL Server Management Studio) and connect to the RequestCenter database as the RCUser.

Execute the following command:

EXECUTE sp_CleanupSlMessageContent <n>

where <n> = Number of days for which completed/failed Service Link messages are to be retained; -1 means all completed/failed messages will be purged.

At the end of the execution, the total elapsed time should be displayed. Here's an example of the output:

```
Deleting messages with MessageStateID 2 (completed) or 3 (failed) that are older than 100
days

Deletion of messages started at Jul 6 2011  2:57PM

Done deleting 1530 messages Jul 6 2011  2:58PM
```

Manage Integrations

The complete reference of Service Portal integration points is available in the *Cisco Service Portal Integration Guide*. This section provides an overview of the key integration strategies that the system administrator may pursue when configuring the Service Portal application.

Integration Types

The following types of integrations are supported:

Data-level Integration using Directory Integration

Synchronization of data between Service Portal and an LDAP directory.

For example: Organizational Structure, Exchange Calendar Info.

Application-level Integration using Single Sign-On

Single Sign-On allows users to bypass the login screen and access Service Portal directly from a portal or other application.

Form-level Integration using Interactive Service Forms (ISF) and Active Form Rules

JavaScript functions interact with third-party systems to collect, validate, or distribute form information and to adjust the appearance or behavior of the form dynamically.

For example: Cost Code Validation, Auto-Population of Fields.

Task-level Integration using Service Link

Service Link provides asynchronous messaging using HTTP, file, database, MQ and JMS adapters. External tasks trigger Service Link agents to issue a command to another system and expect a response.

For example: Open a Help Desk Ticket, Update an Asset, Order Equipment.

Requisition-level Integration using Web Services RAPI

A third-party application initiates an action within Request Center using Requisition API (RAPI).

For example: Canceling a pay check in a financial system causes Request Center to initiate and manage an Off-Boarding Process to disable accounts and reclaim assets.

Directory Integration

The system allows for multiple LDAP directory integrations. A group of two or more LDAP sources becomes one LDAP system through referrals. For detailed information on configuring directory integrations, please consult the *Cisco Service Portal Integration Guide*.

Directory Integration allows integration architects to connect Service Portal to an LDAP data source and map attributes in that data source to corresponding fields in the Person profile. The integration allows designers to designate which events should trigger an LDAP lookup, and whether that lookup should also cause a refresh of the Person profile in Service Portal. Events that can trigger an LDAP lookup include:

- Authentication after login, either via the Service Portal screen or Single Sign-On
- Person Search for Order On Behalf
- Person Search for form data in a Person-type field
- Lookup of Person information for the manager(s) of a person previously selected via Order on Behalf or Person Search

In addition to these pre-configured events and behavior, Directory Integration provides an API to allow programmers to implement custom directory interfaces to add new search capabilities or refine the search logic.

Directory Mappings

Directory data can be mapped to elements of a Person's profile including

- Basic and extended person attributes, including location and contact information
- One or more organizations
- One or more groups
- One or more roles

Four types of mappings are available:

- Simple mapping. A 1-to-1 mapping between a directory attribute and a Person field.

- Composite mapping. Two or more directory attributes are used to derive the value of a Person field.
- Expression mapping. A regular expression involving one or more directory attributes is used to conditionally derive the value of a Person field.
- Mapping via Java class, using the Directory Integration API. A Java plug-in derives the value of the Person field based on directory attributes available in the current directory data source for the current person.

If the Locale and Time Zone are not mapped, Service Portal uses the server default.

If any optional fields are not mapped, any value previously populated in the Person profile will remain unchanged.

Custom Mappings

Custom mappings can be created via pattern-matching language (regular expressions), which is described in the *Cisco Service Portal Integration Guide*, and via a custom plug-in class based on an interface provided in the Directory Integration API.

Any such mappings should be documented in the LDAP Integration document for each implementation. Any Java classes required for the mapping are treated as customizations if/when a Service Portal instance is migrated or upgraded.

Custom Code

Using the interfaces provided by the Directory Integration API, custom Java classes can replace or supplement the pre-configured behavior offered by the directory integration events. Any such classes are treated as customizations when/if an instance is migrated or upgraded.

Further, if the custom classes require supporting JAR files, these must be installed on the application server and treated as customizations. Installation procedures differ for each application server:

WebSphere

Step 1 Copy third-party JARs to a folder outside of WAS.

Step 2 In WAS console, go to **Environment > Shared Libraries**. Browse to the **Cell** scope. This ensures the libraries are seen by all entities in the Cell. (You may change the scope as required.) Click **New**, enter a reference name to the JAR, and in Classpath, enter the full path to the JAR; do this for each JAR. Save your changes.

Step 3 Go to **Applications > Enterprise Applications**, and select your application. In Configuration tab, go to **Additional Properties > Libraries**. Click the **Add** button and add each library that you created. Save your changes and restart the application.

JBoss

Step 1 Add the third-party JARs to RequestCenter.ear\ folder.

Step 2 Add a module reference for each of the third-party JARs in RequestCenter.ear\META-INF\application.xml.

Step 3 Restart the Request Center service.

Single Sign-On

Single Sign-On functionality is provided as part of Directory Integration.

Single Sign-On Troubleshooting

If you experience any problems with Single Sign-On, begin troubleshooting by checking the following items:

- Review any related changes to your environment such as LDAP or Junction/SiteMinder agent configurations.
- Can you still access Service Portal via the Administrative override?
- Restart the Request Center service.

Single Sign-On: Configuring NTLM

Many environments use Windows authentication. IIS supports Integrated Windows Authentication (IWA) and passes the DOMAIN\UserName of the user who is logged in as a parameter.

Requirements

- Restart the IIS Admin Service (in Windows Services) after enabling IWA
- Valid domain accounts while accessing Service Portal
- Configure SSO to strip DOMAIN information

Interactive Service Forms (ISF)

ISF is a JavaScript API that integrates with Request Center service forms. ISF allows the forms to dynamically alter their contents or behavior based on the current context, including the user's credentials; data previously entered on the form; or the life cycle of the requisition displayed. For more information on ISF, please consult the *Cisco Service Portal Designer Guide*.

ISF supports the use of JavaScript libraries, stored on the application or web server, to supplement JavaScript code stored in the Service Portal repository. If such libraries are used, they are treated as customizations when upgrading or migrating a Service Portal site.

Active Form Rules

The data retrieval rules available within active form components allow Request Center to retrieve data from external relational databases or from the application database, for use in service forms. Such data can be used to pre-fill form fields with default values; to produce drop-down lists; and to provide dynamically populated drill downs to detailed information. User data entry could also be validated against the external data.

For a rule to access an external database, a corresponding JEE datasource must be created. Instructions on creating the datasource are given in the *Cisco Service Portal Installation Guide*. Any such datasources are treated as customizations when upgrading or migrating the Service Portal site.

Service Link

Service Link, also known as the Integration Server, or ISEE (Integration Server Enterprise Edition), allows Request Center to send synchronous or asynchronous requests to other systems via XML messages.

Tasks that are configured in Service Designer as "external" are handled by Service Link.

Service Link uses JMS queues as an underlying technology, so disruption to JMS configuration may disrupt Service Link operation. Most Service Link troubleshooting can be done through the Service Link module which provides the ability to drill-down to individual messages sent or received and the tasks responsible for sending or receiving those messages.

Including Custom Content during Installation

Overview

This section provides information about configuring your system for a customized installation of Service Portal, and for ensuring that custom content is not deleted or overridden during subsequent installations or upgrades.

For more details on the Installer, please consult the *Cisco Service Portal Installation Guide*.

How the Installer Works

The Installer builds the EARs and:

- Expands the core product EAR
- Modifies .properties files based on settings selected during installation
- Merges in a customizations file, if one is specified as part of the installation parameters
- Re-jars the EAR
- Publishes the EAR to the dist/folder for deployment (for WebSphere and WebLogic)

The deployment procedure stipulates that an entire EAR file be deployed to a server. When an entire EAR file is deployed, the previous directory where the EAR was expanded is wiped clean, and any Service Portal customizations that existed in the directory are lost.

Including Custom Content during Installation

To avoid losing the customizations, the Installer allows you to specify custom content to be included in the installation:

Step 1 Create an archive containing the custom content. The archive's directory structure must match the deployment directory structure.

Step 2 Run the installer as described in the *Cisco Service Portal Installation Guide*, and complete all the steps until the **Options** screen appears.

```
Site Component Installation Options

  11.  Webserver Type                 IIS
  12.  Configure Webserver            Yes
  13.  Website Instance Name          Default Web Site
  14.  Webserver Host                 vmhw21.oakqas.celosis.com
  15.  Webserver Port                 80
  16.  Use Local DTD                  No
  17.  AppServer JNDI Port            4099
  18.  Cluster Request Center         No
  19.  Include custom content?        No
  20.  Install as Service?            No
```

Step 3 Select the **Include custom content?** option.

Step 4 Press **Y** to confirm that you want to include custom content.

The Custom content archive path option appears beneath the Include Custom Content? option.

```
Site Component Installation Options

  11.  Webserver Type                 IIS
  12.  Configure Webserver            Yes
  13.  Website Instance Name          Default Web Site
  14.  Webserver Host                 vmhw21.oakqas.celosis.com
  15.  Webserver Port                 80
  16.  Use Local DTD                  No
  17.  AppServer JNDI Port            4099
  18.  Cluster Request Center         No
  19.  Include custom content?        Yes
(*)20.    Custom content archive path
  21.  Install as Service?            No
```

Step 5 Select the **Custom content archive path** option.

The Installer prompts you to enter the path to the archive.

Step 6 Enter the full path to the archive, including the name of the archive.

Step 7 Continue with the installation as described in the *Cisco Service Portal Installation Guide*.

While the Installer completes the installation, it extracts your custom content archive into the application deployment directory structure.

A similar installation option is available for installing any custom Service Link adapters, built using the Service Link Adapter Development Kit (ADK), or one of the Service Adapter Kits. This option is described in detail in the "Installing Additional Service Link Adapters" section on page 5-38.

Implementation-Wide Custom Files

All customized files should be included in the customization archive. The following customized files may be required at all sites within an implementation:

Customizable Component	Directory/Files
Custom style sheets, headers, footers	RequestCenter.war\custom*\custom.css RequestCenter.war\custom*\portal-custom-header.css RequestCenter.war\custom*\images\ RequestCenter.war\custom*\header.html, footer.html, for all directories on which custom style sheets have been installed
ISF libraries	RequestCenter.war\isfcode*
Custom Classes	RequestCenter.war\WEB-INF\classes\ (custom classes such as those related to Directory Integration customization)
Property Files edited by hand (such changes could also be site-specific)	newscale.properties integrationserver.properties be.properties xml4j.properties (logging)

Site-Specific Custom Files

Some customized content may be specific to the site or environment. To allow ease of upgrades within different environments, the build script can track environment-specific files.

Any changes to the following configurations are not propagated without modifying the appropriate file:

Customizable Component	File(s)
ColdFusion DataSource configuration	neo-query.xml
ColdFusion Administrator password	password.properties

Database Scripts

Modifying the database outside of the APIs provided by Cisco is strongly discouraged. However, some scripts may need to be executed directly against the database.

External Dictionaries

External Dictionaries are stored as database tables. Whenever these dictionaries are modified, DDL scripts need to be run to modify the corresponding table.

Patches

Customer Support may provide a SQL script as part of a patch or hotfix that needs to be run manually. Until a hotfix is included in a subsequent product release, it must be treated as a customization to be included in a software upgrade or re-install.

Catalog Deployer and Configuration Management

A Service Portal implementation typically consists of multiple sites, each of which plays a different role:

Site	Usage
Development	Service definitions are developed and unit tested; customizations are initially applied
Test	A controlled environment, not interrupted by development activities, where Quality Assurance or other personnel test a service catalog
Production	The live environment where the user community can request services from the service catalog and IT teams can fulfill service requests

The previous portion of this chapter discussed management of configuration items that reside outside of the Service Portal repository. Following the guidelines above will allow you to upgrade Service Portal software without losing the customizations you have applied to that software. However, these guidelines do not address the need to migrate client-provided content—for example, service definitions and Person profiles—from one site to another. That capability is provided by Catalog Deployer.

The Catalog Deployer module provides configuration management for metadata (service definitions) and organizational data (people, organizations, and related entities) which is stored in the repository.

Recommended Process for Copying a Database

At certain times during a deployment, it may be desirable to copy the Service Portal OLTP database from one site to another. For example:

- When initially installing a test or production site, the complete development site may be copied to the new environments.
- After production has been in operation for a time, all of the user activity should be copied to a test environment, to allow realistic performance or volume studies.

Follow the procedures below to copy a Service Portal OLTP database from one site to another.

Export Source

Step 1 Inform the users of expected downtime.

Step 2 Stop the Request Center and Service Link services in the source environment.

Step 3 Export the source database. Develop a naming convention that allows you to track the source of the data and the date of the export.

Step 4 If a system shutdown is not feasible, use the –consistent flag for the Oracle export.

Step 5 Restart the Request Center and Service Link services.

Import to Target

Step 1 Stop the Request Center and Service Link services in the target environment.

Step 2 Ensure you have a current backup copy of the target database.

Step 3 If required, copy the export file from its destination to a file system accessible to the target database server.

Step 4 Import data into the target database.

Step 5 For SQLServer, ensure that logins and users exist in the newly imported database match the credentials required for this instance of Service Portal. If required, create a new login and/or associate an existing login with the database owner and ensure this user has appropriate permissions. For Oracle, ensure appropriate users exist in the newly imported database with privileges as specified in the Service Portal installer.

Step 6 If the two sites are accessing two different Cognos reporting servers, update the entry in the CnfParams table that specifies the name of the "CognosServer" for this site and commit the update.

Step 7 Restart the Request Center and Service Link services in the target environment.

Step 8 Set the **Administration > Entity Homes > SiteProtection** "This Site Is" property to the current site. If Entity Homes are specified differently, or sites have different protection levels, make the changes manually and save your changes.

Step 9 If the two sites are connecting to two different LDAP directories, adjust the Directory Integration Data Source definition appropriately.

Step 10 Check and modify any connection properties for the Service Link agents as appropriate for the target environment.

Step 11 Perform any additional manual operations to adjust the data. For example, you may wish to add permissions to some people, groups, or organizations, or revoke permissions.

Step 12 Inform users that maintenance is complete.

Installing Additional Service Link Adapters

Overview

Service Link ships with several default adapters. To augment the set of default Service Link adapters, customers may create custom adapters, or purchase Service Adapters designed to work with Service Link. This section describes how to install customer-created custom adapters and Service Link Service Adapters when installing the Service Portal.

Installing Additional Service Link Adapters

To install Advanced Services adapters or custom adapters during installation:

Step 1 Obtain the adapter archive from Cisco Advanced Services and copy it to your hard disk, or create an archive containing the custom Service Link adapter and copy it to your hard disk. See the *Cisco Service Portal Integration Guide* for more information about custom adapters.

Step 2 Run the installer as described in the *Cisco Service Portal Installation Guide*, and complete all the steps until the **Options** screen appears.

Step 3 Select the **Include Custom Adapters?** option.

Step 4 Press **Y** to confirm that you want to include a custom Service Link adapter.

The Custom adapter archive path option appears beneath the Include Custom Adapter? option.

Step 5 Select the Custom adapter archive path option.

The Installer prompts you to enter the path to the archive.

Step 6 Enter the full path to the archive, including the name of the archive.

Step 7 Continue with the installation as described in the *Cisco Service Portal Installation Guide*.

While the Installer completes the installation, it extracts your custom content archive into the application deployment directory structure.

Step 8 Repeat these steps for each additional Service Link adapter you wish to install. You cannot install multiple additional Service Link adapters at once.

Configuring SSL for Service Link Inbound Documents

Overview

Enabling SSL for the Service Link service involves:

- Getting a digital certificate that is either self-signed or signed by a known CA such as VeriSign.
- Installing the certificate, and
- Configuring a secure port number for the application server on which the Service Link service is running.

Procuring a certificate signed by a well-known Certificate Authority like VeriSign or Thawte has the benefit that most client programs already recognize the signer certificate from one of these Certificate Authorities. If you choose to use a self-signed certificate for your Service Link service, then you must exchange the signer certificate with all external systems that communicate with Service Link via web interface. For example, if an external system sends a response message to a Service Link agent which uses the http/ws adapter for its inbound adapter, then that external system acts as a client that connects to Service Link via an **https** URL, and will need to understand how to complete the trusted handshake for a successful SSL connection. In order to do this, the external system needs to recognize the signer for the certificate used by the Service Link service. To achieve this, the signer certificate for Service Link must be imported into the *Trusted Certificate Authority Keystore* of the external system. More detailed instructions are given later in this chapter.

Note Service Link, as a server, does not support client certificate authentication during SSL handshake.

Secure vs. Non-Secure Port

Enabling SSL for Service Link turns on the secure port, but it does not turn off the non-secure port for Service Link. If you choose not to turn off the non-secure port, external systems can still communicate with Service Link via an http URL. If you decide to turn off the non-secure port, all communications with the Service Link service must use the **https** URL.

It is possible to use both secure and non-secure port for the Service Link service and control the access to the non-secure port via another mechanism, such as a firewall system. For example, in JBoss environments, the Request Center application is also a "client" of the Service Link service (which runs on a separate JBoss server). At runtime, Request Center needs to connect to the Service Link service via the URL http://<*SL_servername*>:8089. If the non-secure port 8089 is turned off for the Service Link service, then Request Center must be configured to connect to Service Link via an https address, that is, **https**://<*SL_servername*>:**8443**. So, one possible scenario is that you turn on both non-secure port 8089 and secure port 8443 for the Service Link service. Request Center can still connect to Service Link via http://<*SL_servername*>:8089, while other external systems must only communicate with Service Link via https://<*SL_servername*>:8443. You configure your firewall system to deny access to port 8089 from all external systems.

This section does *NOT* describe how to turn off a non-secure port for the application server or how to configure a firewall system to deny access to a non-secure port number. Please contact your system administrator, or the vendor of your application server product to obtain the information you need.

Clustered vs. Non-Clustered Environment

In a JBoss environment, Service Link runs on a separate JBoss server. To enable SSL for Service Link, you will configure the certificate and secure port number for the JBoss server where Service Link is running.

In a non-clustered WebLogic/WebSphere environment, Service Link is deployed in the same WebLogic/WebSphere server as the Request Center application. To enable SSL for Service Link, you will in effect configure the certificate and secure port number for the same WebLogic/WebSphere server that services both Service Link and Request Center.

In a clustered WebLogic/WebSphere environment, Service Link must be deployed in a separate WebLogic/WebSphere server that does not belong to the cluster. (Only Request Center and the Business Engine are deployed in the cluster.) Thus, to enable SSL for Service Link, you will configure the certificate and secure port number only for the WebLogic/WebSphere server where Service Link is running.

Creating a Certificate Keystore

It is assumed that you have managed to procure a digital certificate that can be used to secure the Service Link service. This certificate can either be self-signed or obtained through a third-party Certificate Authority like VeriSign. In either case, your digital certificate must be imported into a java keystore (that is, a jks file) that can be accessed by the application server. Furthermore, the signer certificate (aka the public key of your certificate) must be exported into a file in "Base64-encoded ASCII" format, so that it can be given to the external systems that want to communicate with Service Link service in SSL mode.

The instructions in the rest of this document assume that you start with a valid keystore file that already contains your digital certificate. For ease of documentation, let's assume that your keystore file is named "**slkeystore.jks**". It contains a certificate under the alias called "**servicelink**". The password to open this keystore file is "**slpassword**".

Let's also assume that the signer certificate has been exported in "Base64-encoded ASCII" format into a file named "**slsigner.ce**r". A "Base64-encoded ASCII" format may look like the following example:

```
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCBE17w1cwDQYJKoZIhvcNAQEEBQAwZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNB
MRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG51d1NjYWxlMQswCQYDVQQLEwJRQTEVMBMG
A1UEAxMMS2hhbmcgTmd1eWVuMB4XDTExMDMxMjE5MDI0N1oXDTIxMDMwOTE5MDI0N1owZTELMAkG
A1UEBhMCVVMxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG51d1Nj
YWxlMQswCQYDVQQLEwJRQTEVMBMGA1UEAxMMS2hhbmcgTmd1eWVuMIGfMA0GCSqGSIb3DQEBAQUA
```

```
A4GNADCBiQKBgQDhTxg2RwarD6Wn4iqYeOOk3ykfXzZiDArf/X63omXquTmN0Up+mg6oJmPAfqJA
l7k4+Dn7dfVtAc4h8qra7PBeBU48zrzRqZd6VAK07rz++CilQto64mHXYVomb5vWPGeKA41j9vlv
ENj/tE/6++IqbwnxAqeZtY3EvEM7dcCWDwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAAaqCnfEAovy
Uf2S+oAXYDo5N387a035APsz5iiUM5oiKR/KW3oRz/v0P0I/o3n312kDIJ01111pl6qpZRtPEsr1
b00Tu1cXfPmizEtz0ole606qDS+DzkS1+YYz2mLL2Zq40d1EPsMolyqyUmyq3GHaEnuhWemcv2aA
wGFgbQYd
-----END CERTIFICATE-----
```

Installing the Keystore for the Application Server

The subsequent sections contain instructions for installing the certificate file and configuring SSL for each type of application server.

JBoss 4.2.3

Perform the following steps as the "administrator" user of the Service Link machine.

Step 1 Copy the certificate keystore file "slkeystore.jks" to the "<APP_HOME>\jboss-4.2.3.GA\server\ServiceLink\conf" directory on the Service Link machine.

Step 2 Modify file "<APP_HOME>\jboss-4.2.3.GA\server\ServiceLink\deploy\jboss-web.deployer\server.xml" as follows.

Search for the following section:

```
<!—
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

and change to: (*Remove the comment brackets, and add the keystoreFile and keystorePass variables. Use forward-slash instead backslash in the directory path.*)

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:/CiscoServicePortal/jboss-4.2.3.GA/server/ServiceLink/conf
/slkeystore.jks"
keystorePass="slpassword" />
```

Step 3 Make sure port 8443 is not used on your machine. If it's already used, then change the "Connector port" to another port number that is available.

Step 4 Restart the Service Link service.

Step 5 Look in the log file "<APP_HOME>\jboss-4.2.3.GA\server\ServiceLink\ log\server.log" for the following message to ensure that the ServiceLink service has started up in port 8443:

```
INFO  [org.apache.coyote.http11.Http11Protocol] Starting Coyote HTTP/1.1 on http-8443
```

Your Service Link service is now SSL-enabled.

Step 6 Skip this step if you have already created the file "slsigner.cer" that contains the signer certificate for the *servicelink* certificate. Otherwise, perform the following procedure to export the signer certificate. There are several methods to export the signer certificate; the following procedure is just one way to do it using the "keytool.exe" utility that comes with the Sun JDK 6 installation.

a. Execute the following commands on a Command Prompt window:

```
cd <APP_HOME>\jboss-4.2.3.GA\server\ServiceLink\conf
<JAVA_HOME>\bin\keytool -export -rfc -file slsigner.cer -alias servicelink -keystore
slkeystore.jks -storepass slpassword
```

b. To verify that the file "slsigner.cer" is good, execute:

```
<JAVA_HOME>\bin\keytool -printcert -file slsigner.cer
```

Step 7 If you decide to disable the non-secure port (8089) for the Service Link service, send the file "slsigner.cer" to the system administrator who manages the external system which communicates with the Service Link service. Two things need to be configured for that external system:

a. The Service Link URL needs to be changed from an http address to an **https** address with the secure port number. For example, previously, the Service Link URL may have be:

```
http://<sl_servername>:8089/IntegrationServer/ishttplistener/ <agent_name>
```

It must now be changed to:

```
https://<sl_servername>:8443/IntegrationServer/ishttplistener/ <agent_name>
```

b. The signer certificate of the *servicelink* certificate (that is, the contents of file "slsigner.cer") needs to be imported into the *Java Trusted Certificate Authority Keystore* of the external system, so that a trusted handshake can be established during the SSL connection with the Service Link service.

Step 8 If you decide to disable the non-secure port for Service Link, you must also import the signer certificate into the *Java Trusted Certificate Authority Keystore* of the Request Center service. This is because the Request Center application runs on a separate JBoss server and acts as a "client" that connects to the Service Link service at runtime. Complete the following steps to import the signer certificate into the *Java Trusted CA Keystore* for Request Center:

a. Log on to the Request Center machine as the "administrator" user.

b. Locate file "**cacerts**" in the directory "<*JAVA_HOME*>\jre\lib\security", where <*JAVA_HOME*> is the root directory of the Sun JDK 6 installation. This file is the *Trusted CA Keystore* that comes with the Sun JDK 6 installation.

Make sure that <JAVA_HOME> is the correct Java directory used by your JBoss application server. To verify this, look for the JAVA_HOME setting inside the file "setEnv.cmd", located under the "<APP_HOME>\bin" directory. For example: `set JAVA_HOME=C:\jdk1.6.0_23`.

c. Copy the file "slsigner.cert" to the "<*JAVA_HOME*>\jre\lib\security" directory.

d. Import the signer certificate into the "cacerts" keystore by executing the following commands on a Command Prompt window:

```
cd <JAVA_HOME>\jre\lib\security
<JAVA_HOME>\bin\keytool -import -trustcacerts -alias servicelink -noprompt -file
slsigner.cer -keystore cacerts -storepass changeit
```

In the command above, it is assumed that the password for the "cacerts" keystore file is still the default value of "changeit". Replace it with the correct value if the password for "cacerts" has been changed in your environment.

e. Modify the file "**newscale.properties**" under the directory "<APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy\ RequestCenter.ear\config" as follows:

Search for the following parameter:

```
isee.base.url=http://<hostname>:8089
```

and change to:

```
isee.base.url=https://<hostname>:8443
```

f. Restart the Request Center service.

Step 9 To avoid Step 8 entirely, you may decide to turn on both non-secure port 8089 and secure port 8443 for Service Link service. This way the Request Center application can still connect to Service Link using the non-secure URL (http://<*hostname*>:8089). But you may want to consider taking some measures (such as a firewall system) to block access to the non-secure port 8089 from external systems.

WebLogic 10.3

Perform the following steps as a user who can access the WebLogic Administration Console:

Step 1 Copy the certificate keystore file "slkeystore.jks" to the "<*JAVA_HOME*>\jre\lib\ security" directory on the WebLogic machine where Service Link is running.

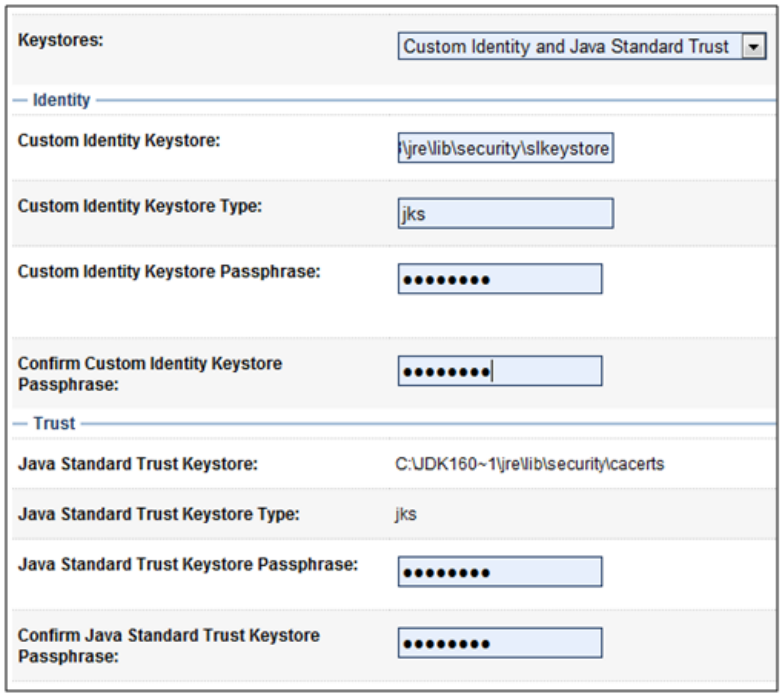
Note In a clustered WebLogic environment, Service Link must be deployed in a WebLogic server that does not belong to the cluster. So, make sure you find the correct WebLogic server for Service Link.

Verify that <JAVA_HOME> is the correct Java directory used by the WebLogic application server. Look for the JAVA_HOME setting inside file "commEnv.cmd" (on UNIX/Linux, look for "commEnv.sh"), located under the "<WL_HOME>\common\bin" directory. For example: `set JAVA_HOME=C:\jdk160_23.`

Step 2 Log on to the WebLogic Administration Console and navigate to ***<domain>*** **> Environment > Servers**.

Step 3 Click the name of the WebLogic server for Service Link to open its configuration settings.

Step 4 Select the **Configuration > Keystores** sub-tab.



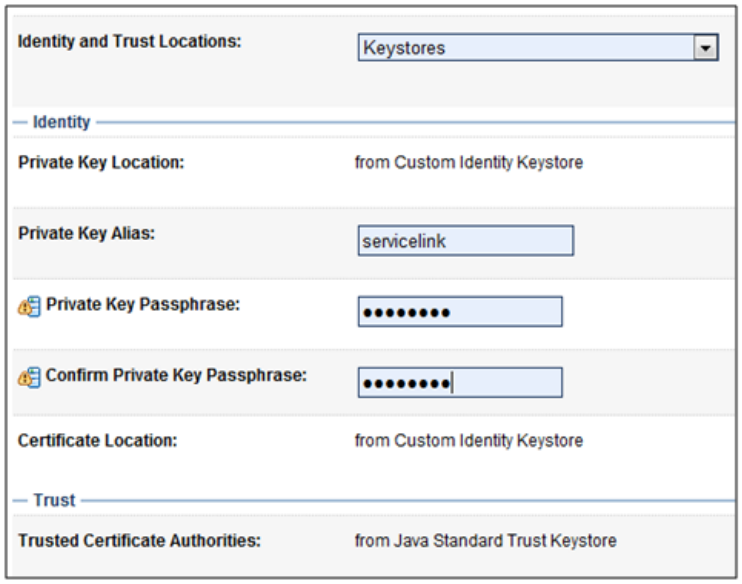
Step 5 On the Keystores page, enter the following values. Replace <*JAVA_HOME*> with the full pathname of the Java Directory. (For the read-only fields, verify that the displayed values are correct.)

Field	Value
Keystores	Custom Identity and Java Standard Trust
Custom Identity Keystore	<*JAVA_HOME*>\lib\security\slkeystore
Custom Identity Keystore Type	jks
Custom Identity Keystore Passphrase	slpassword
Confirm Custom Identity Keystore Passphrase	slpassword
Java Standard Trust Keystore	<*JAVA_HOME*>\lib\security\cacerts
Java Standard Trust Keystore Type	jks
Java Standard Trust Keystore Passphrase	changeit
Confirm Java Standard Trust Keystore Passphrase	changeit

For the Java Standard Trust Keystore Passphrase: It is assumed that the password for the "cacerts" keystore file is still the default value of "changeit". Replace it with the correct value if the password for "cacerts" has been changed in your environment.

Step 6 Click **Save**.

Step 7 Select the **Configuration > SSL** sub-tab.

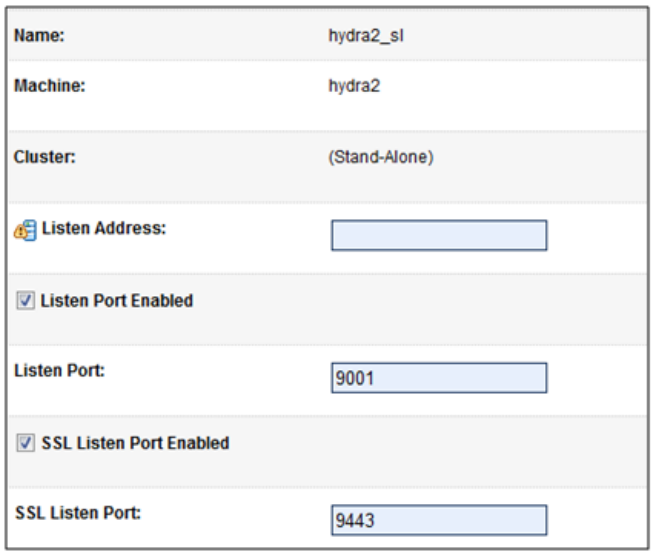


Step 8 On the SSL page, enter the following values:

Identity and Trust Locations	Keystores
Private Key Alias	servicelink
Private Key Passphrase	slpassword
Confirm Private Key Passphrase	slpassword

Step 9 Click **Save**.

Step 10 Select the **Configuration > General** sub-tab.



Step 11 On the General page, enter the following values:

- Select the **SSL Listen Port Enabled** checkbox.
- SSL Listen Port = *<enter an available port number, for example 9443>*.

Step 12 Click **Save**.

Step 13 Restart the WebLogic server where Service Link is deployed.

Step 14 Look in the log file "*<WL_servername>*.out" for messages similar to the following, to ensure that the WebLogic server has started up in the secure port (9443):

```
<Notice> <Security> <BEA-090171> <Loading the identity certificate and private key stored
under the alias hydra2 from the jks keystore file
C:\jdk160_23\jre\lib\security\slkeystore.>
<Notice> <Server> <BEA-002613> <Channel "DefaultSecure" is now listening on
192.168.21.72:9443 for protocols iiops, t3s, ldaps, https.>
```

Your Service Link service is now SSL-enabled.

Step 15 Skip this step if you have already created the file "slsigner.cer" that contains the signer certificate for the *servicelink* certificate. Otherwise, you can perform the following procedure to export the signer certificate. There are several methods to export the signer certificate; the following procedure is just one way to do it using the "keytool.exe" utility that comes with the Sun JDK 6 installation.

a. Execute the following commands on a Command Prompt window:

```
cd <JAVA_HOME>\jre\lib\security
<JAVA_HOME>\bin\keytool -export -rfc -file slsigner.cer -alias servicelink -keystore
slkeystore.jks -storepass slpassword
```

b. To verify that file "slsigner.cer" is good, execute:

```
<JAVA_HOME>\bin\keytool -printcert -file slsigner.cer
```

Step 16 If you decide to disable the non-secure port for the Service Link service, send the file "slsigner.cer" to the system administrator who manages the external system which communicates with the Service Link service. Two things will need to be configured for that external system:

a. The Service Link URL needs to be changed from an http address to an **https** address with the secure port number. For example, previously, the Service Link URL may be:

```
http://<sl_servername>:9001/IntegrationServer/ishttplistener/ <agent_name>
```

It must now be changed to:

```
https://<sl_servername>:9443/IntegrationServer/ishttplistener/<agent_name>
```

b. The signer certificate of the *servicelink* certificate (i.e. the contents of file "slsigner.cer") needs to be imported into the *Java Trusted Certificate Authority Keystore* of the external system, so that a trusted handshake can be established during the SSL connection with the Service Link service.

For a clustered WebLogic environment only

Step 1 If you decide to disable the non-secure port for the Service Link service, then you must also import the signer certificate into the *Java Trusted Certificate Authority Keystore* of the Request Center service. This is because Service Link runs a separate WebLogic server that does not belong to the cluster. (Only Request Center and the Business Engine can be installed on the cluster.) Request Center acts as a "client" that connects to the Service Link service at runtime. Complete the following procedure to import the signer certificate into the *Java Trusted CA Keystore* for Request Center:

a. Log on to one of the nodes of the WebLogic cluster where Request Center application is running.

b. Locate the file "**cacerts**" in the directory "<*JAVA_HOME*>\jre\lib\security", where <*JAVA_HOME*> is the root directory of the Sun JDK 6 installation. This file is the Trusted CA Keystore that comes with the Sun JDK 6 installation.

Make sure that <JAVA_HOME> is the correct Java directory used by your WebLogic application server. To verify this, look for the JAVA_HOME setting inside file "commEnv.cmd" (on UNIX/Linux, look for "commEnv.sh"), located under the "<WL_HOME>\common\bin" directory. For example:

```
set JAVA_HOME=C:\jdk160_23.
```

c. Copy the file "slsigner.cert" to the "<*JAVA_HOME*>\jre\lib\security" directory.

d. Import the signer certificate into the "cacerts" keystore by executing the following commands on a Command Prompt window:

```
cd <JAVA_HOME>\jre\lib\security
<JAVA_HOME>\bin\keytool -import -trustcacerts -alias servicelink –noprompt -file
slsigner.cer -keystore cacerts -storepass changeit
```

In the command above, the password for the "cacerts" keystore file is still the default value of "changeit". Replace it with the correct value if the password for "cacerts" has been changed in your environment.

e. Copy file "cacerts" that you just updated in the last step to the "<*JAVA_HOME*>\jre\lib\security" directory on every node in the WebLogic cluster where Request Center is deployed. For example, if your WebLogic cluster contains three nodes, and each node is a separate machine, then copy the file "cacerts" from this machine to the other two machines.

f. Modify file "**newscale.properties**" under the directory "<*BEA_HOME*>\ user_projects\ domains\<*domain_name*>\servers\<*servername*>\stage\ RequestCenter\config" as follows:

Search for the following parameter:

```
isee.base.url=http://<hostname>:9001
```

and change it to:

```
isee.base.url=https://<hostname>:9443
```

g. Repeat Step (f) for every node in the WebLogic cluster where Request Center is deployed.

h. Restart the WebLogic cluster for Request Center.

Step 2 To avoid Step 1 entirely, you may decide to turn on both the non-secure and secure ports for the Service Link service. This way the Request Center application can still connect to Service Link using the non-secure URL (http://<*hostname*>:9001). But you may want to consider taking some measures (such as a firewall system) to block access to the non-secure port from all external systems.

WebSphere 7

At installation time, the WebSphere setup program automatically configures both the non-secure port (*WC_defaulthost*) and secure port (*WC_defaulthost_secure*) for your WebSphere server. It also automatically installs a self-signed certificate (with a 1-year expiration date) under the alias named "**default**" for your WebSphere server. You can choose to do one of the followings:

- Use the "*default*" self-signed certificate for your WebSphere server where Service Link is running.
- Use the certificate in the "slkeystore.jks" file that you created at the beginning of this chapter, or
- Create another self-signed certificate for your WebSphere server.

This document does NOT describe how to create a self-signed certificate for your WebSphere server. However, the subsequent sections contain the instructions for the following: a) how to use the existing "*default*" certificate, or b) how to use the certificate in the "slkeystore.jks" file.

Before selecting which certificate to use, you must first perform the steps described in the next section to find out what the secure port number and what keystore are used by the WebSphere server on which Service Link is running.

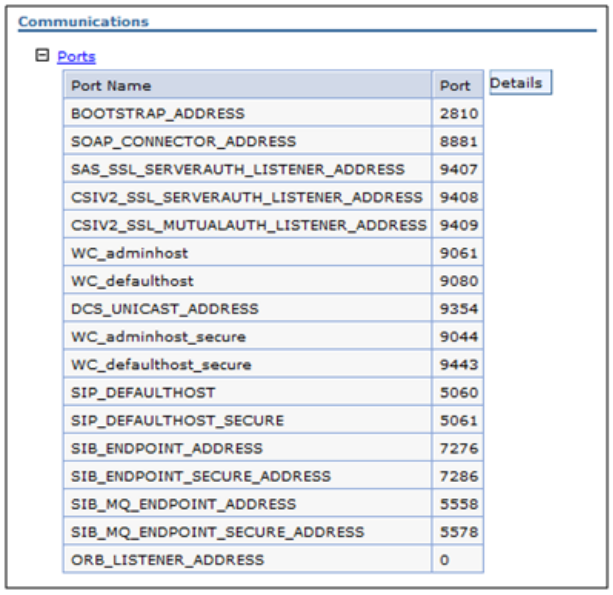
Locating Secure Port Number and Keystore for WebSphere Server

Step 1 Log on to the WebSphere Administration Console, and navigate to **Servers > Application servers**.

Step 2 Click on the name of your WebSphere server where Service Link is deployed.

In a clustered WebSphere environment, Service Link must be deployed in a WebSphere server that does not belong to the cluster. Make sure you find the correct WebSphere server for Service Link.

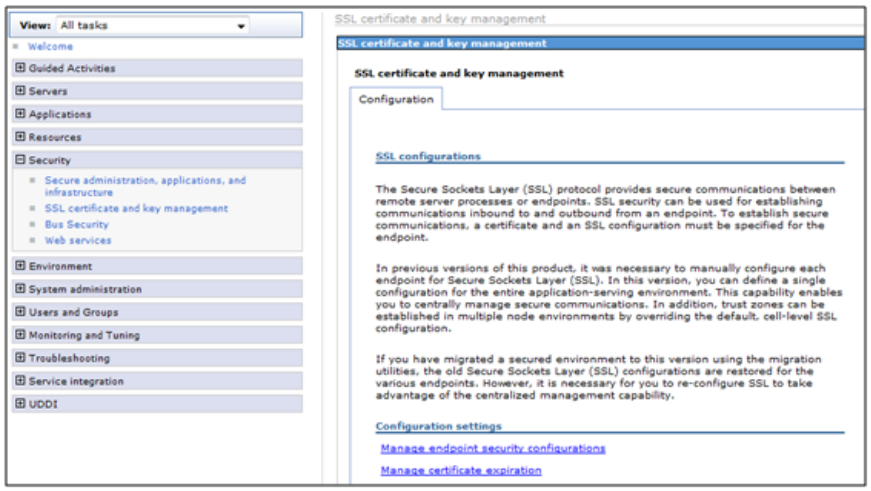
Step 3 On the Configuration tab, expand the "Ports" node.



Port Name	Port
BOOTSTRAP_ADDRESS	2810
SOAP_CONNECTOR_ADDRESS	8881
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS	9407
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS	9408
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS	9409
WC_adminhost	9061
WC_defaulthost	9080
DCS_UNICAST_ADDRESS	9354
WC_adminhost_secure	9044
WC_defaulthost_secure	9443
SIP_DEFAULTHOST	5060
SIP_DEFAULTHOST_SECURE	5061
SIB_ENDPOINT_ADDRESS	7276
SIB_ENDPOINT_SECURE_ADDRESS	7286
SIB_MQ_ENDPOINT_ADDRESS	5558
SIB_MQ_ENDPOINT_SECURE_ADDRESS	5578
ORB_LISTENER_ADDRESS	0

Step 4 Find out what port numbers are configured for "**WC_defaulthost**" and "**WC_defaulthost_secure**". The port number for "WC_defaulthost" is the non-secure port, and the one for "WC_defaulthost_secure" is the secure port. Write down the secure port number as you will need it later.

Step 5 Navigate to **Security > SSL certificate and key management**.

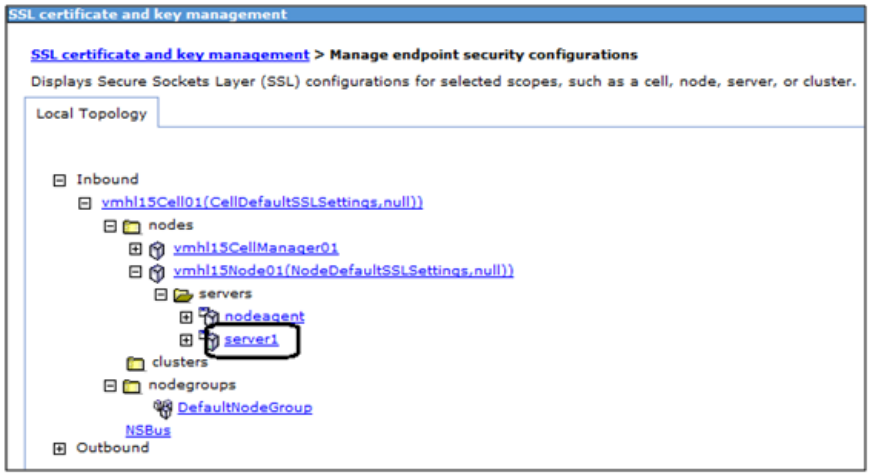


Step 6 Click **Manage endpoint security configurations**.

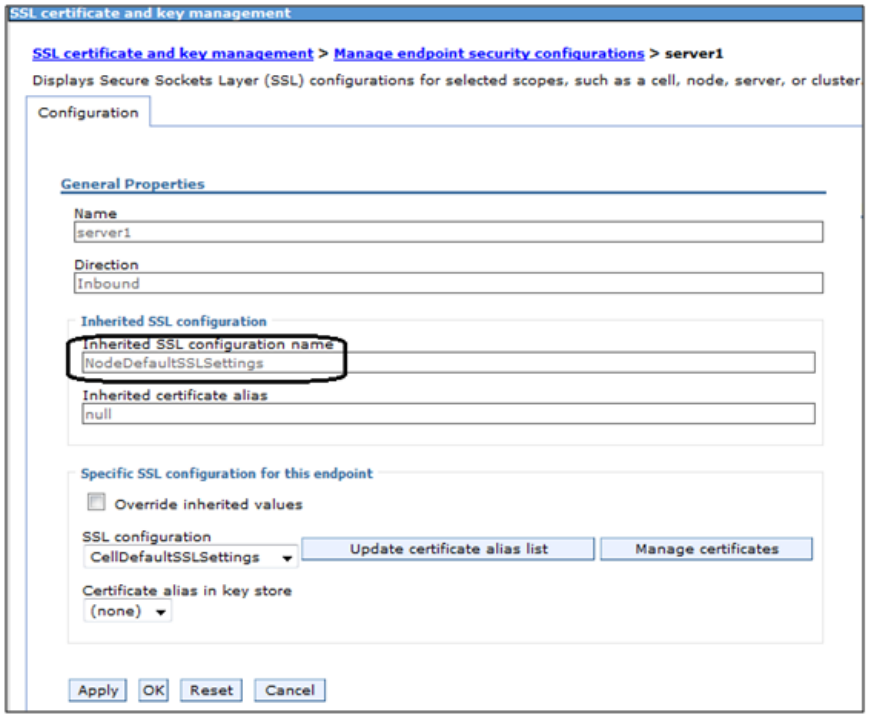
Step 7 Expand "**Inbound > <*cell_name*> > nodes > <*node_name*> > servers > <*SL_server*>**", where <*SL_server*> is the WebSphere server on which Service Link is deployed.

Note In a clustered WebSphere environment, Service Link must be deployed in a WebSphere server that does not belong to the cluster. So, make sure you find the correct server for Service Link.

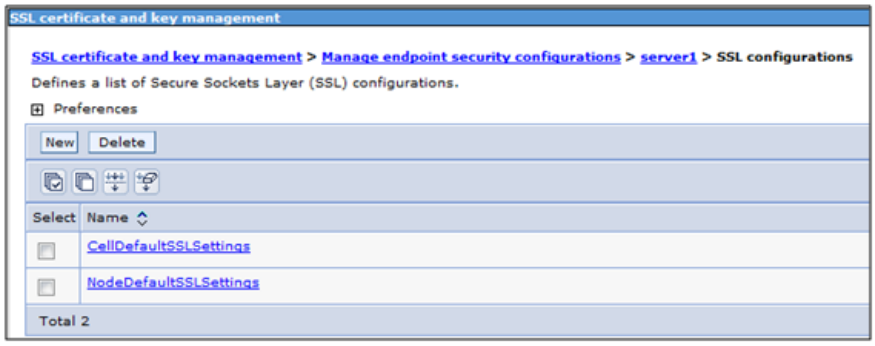
The following screenshot and the rest of the screenshots in this section are only examples. Your WebSphere environment will look different with regards to <cell_name>, <node_name> and <SL_server>.



Step 8 Click on the ***<SL_server>*** link to open its configuration page. Find out what is displayed in the "Inherited SSL configuration name" field. For example, in the screenshot below, the "Inherited SSL configuration name" field is set to the value "NodeDefaultSSLSettings".

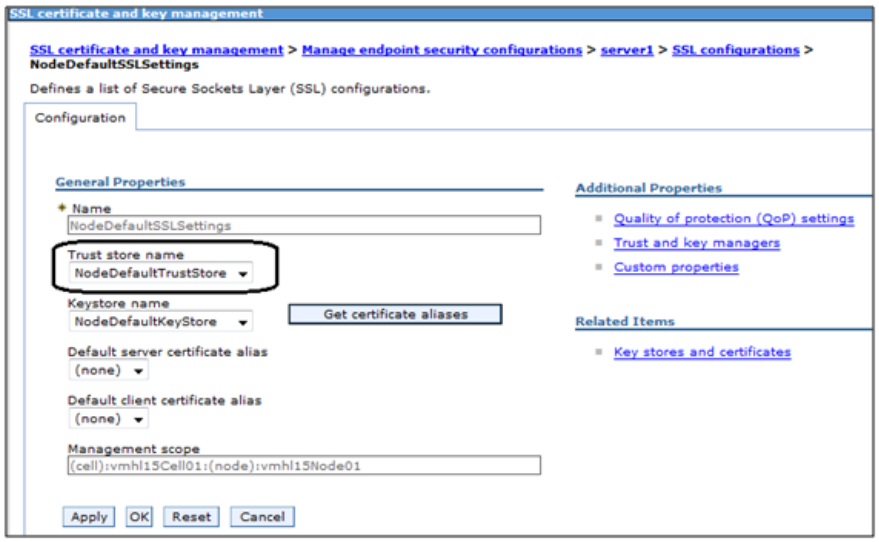


Step 9 Under the Related Items section on the right-hand side, click on **SSL configuration**, then click on **NodeDefaultSSLSettings**.



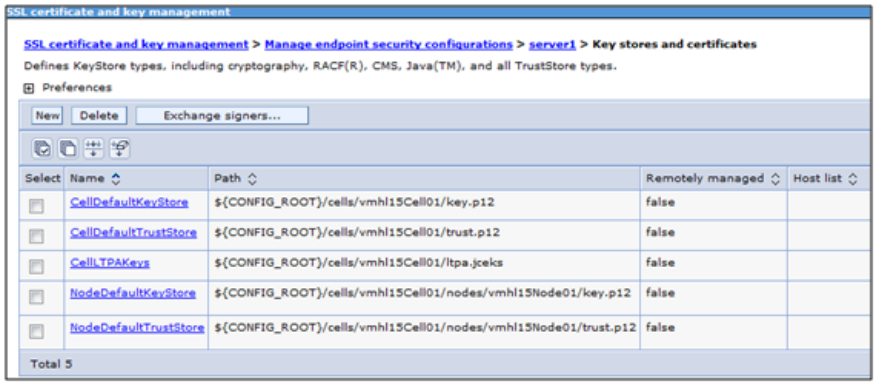
Step 10 On the NodeDefaultSSLSettings page, set the following values, then click **OK**:

Field	Value
Trust store name	NodeDefaultTrustStore
Keystore name	NodeDefaultKeyStore

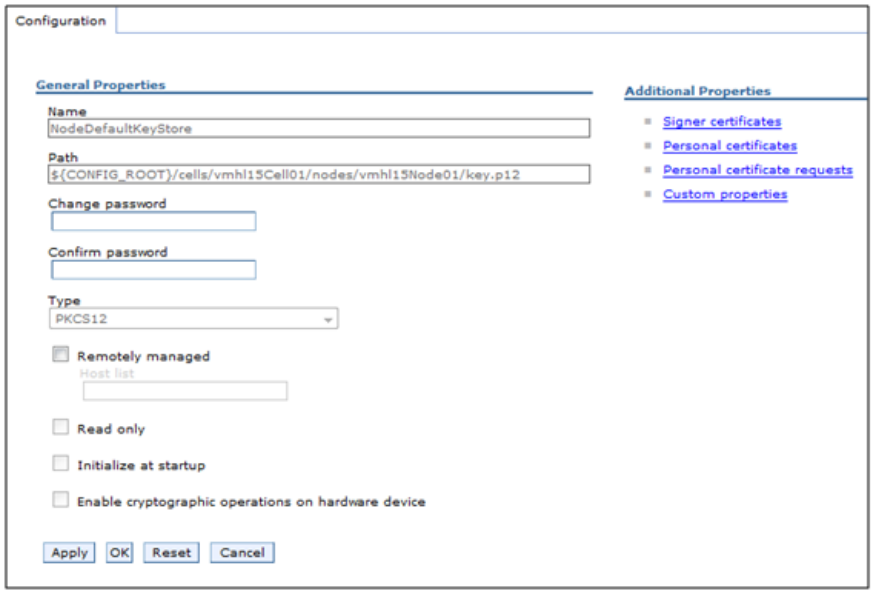


Step 11 Click **Save directly to the master configuration**.

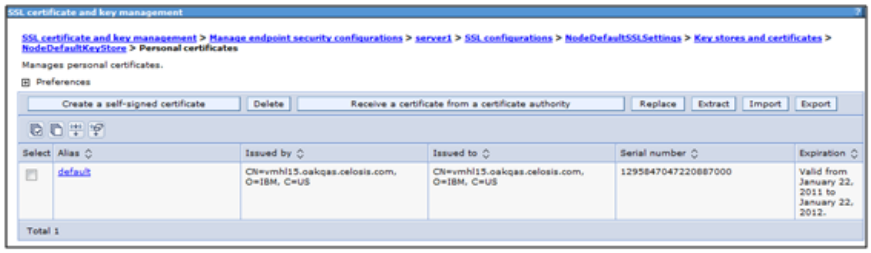
Step 12 Re-open the "NodeDefaultSSLSettings" page again (as seen in the above screenshot), and click on **Key stores and certificates** under the Related Items section on the right-hand side.



Step 13 Click on **NodeDefaultKeyStore**.



Step 14 Click on **Personal certificates** under the Additional Properties section.



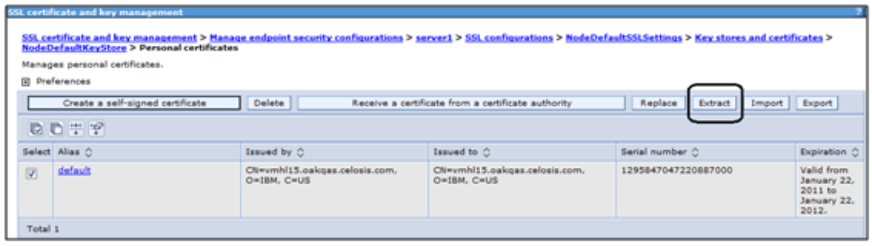
Step 15 Look for the alias "*default*", and verify that the certificate has not expired.

Step 16 If the "*default*" certificate has not expired and you want to use it for your Service Link service, then proceed to the "Using the "default" certificate" section below.

Step 17 On the other hand, if you decide to use the certificate that you created in file "slkeystore.jks" at the beginning of this section, then skip to "Using the "slkeystore.jks" file".

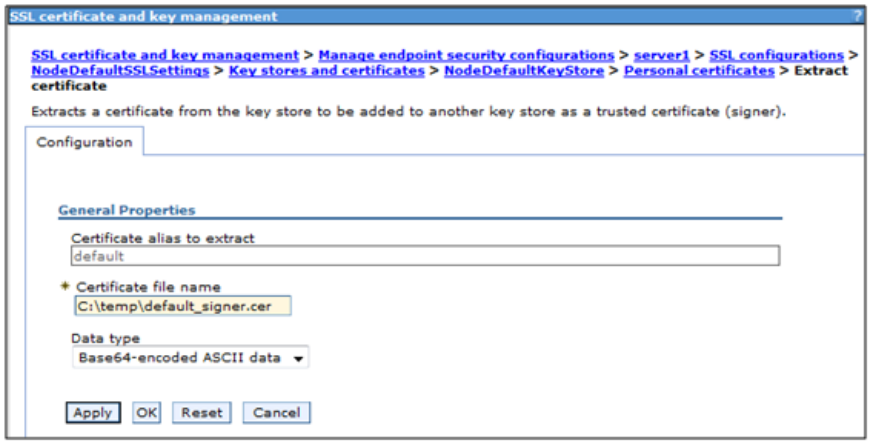
Using the "default" certificate

Step 1 On the Personal certificates page, select the checkbox in front of "*default*" alias, then click the **Extract** button.



Step 2 Enter the following values:

Field	Value
Certificate alias to extract	default
Certificate file name	Enter a pathname such as *C:\temp\default_signer.cer>*
Data type	Base64-encoded ASCII data



Step 3 Click **OK**.

Step 4 Restart the WebSphere server where Service Link is deployed.

Step 5 Look in the log file "SystemOut.log" for messages similar to the followings, to ensure that the WebSphere server has started up in secure port that is, port 9443):

```
TCPC0001I: TCP Channel TCP_4 is listening on host *  (IPv4) port 9443.
CHFW0019I: The Transport Channel Service has started chain WCInboundDefaultSecure.
```

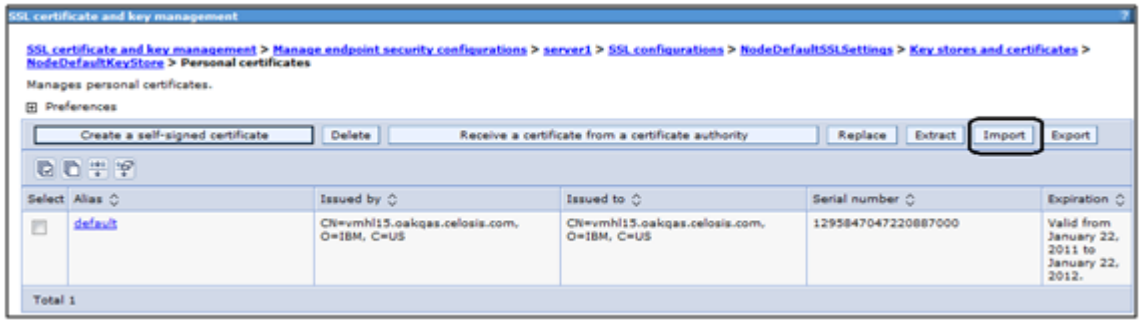
Your Service Link service is now SSL-enabled, and is using the "*default*" certificate.

Step 6 If you decide to disable the non-secure port for the Service Link service, send file "C:\temp\default_signer.cer" to the system administrator who manages the external system. This file contains the signer certificate for the "*default*" certificate. It must be imported into the truststore of the external system, so that the external system can establish a trusted handshake with the Service Link service during SSL connection. In addition, the external system needs to connect to the **https** URL of the Service Link service. For example, previously, the Service Link URL may look like "http://<*servername*>:9080/IntegrationServer/ishttplistener/<*agent_name*>". The URL must now be changed to "https://<*servername*>:9443/IntegrationServer/ ishttplistener/<*agent_name*>.

Using the "slkeystore.jks" file

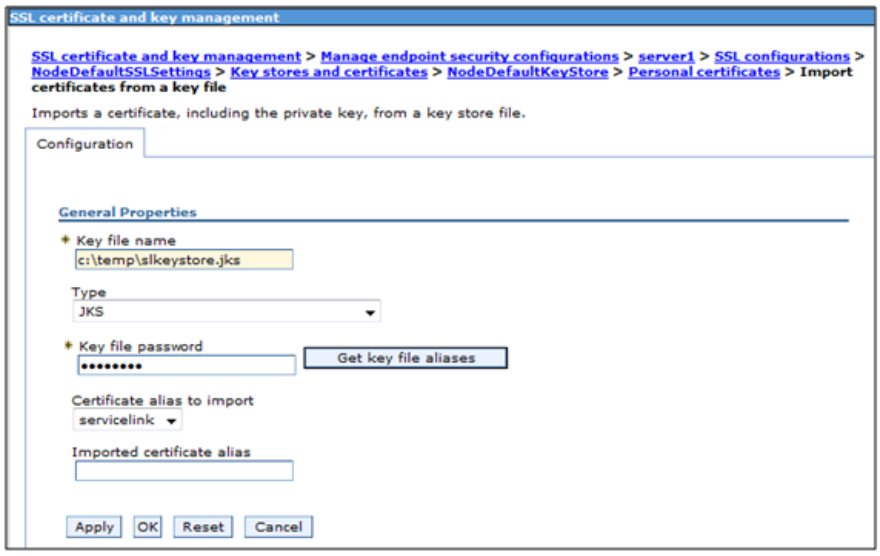
Step 1 Copy file "slkeystore.jks" (that you created at the beginning of this chapter) to a temporary directory on the machine where the WebSphere Administration Server is running. For example, copy the file to C:\temp\slkeystore.jks.

Step 2 On the Personal certificates page, click the **Import** button.



Step 3 Enter the following values:

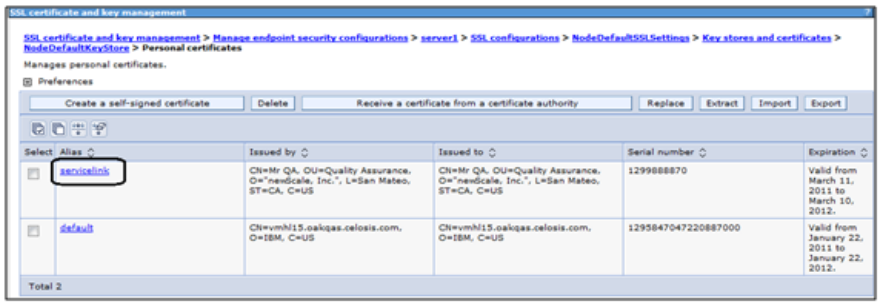
Field	Value
Key file name	C:\temp\slkeystore.jks.
Type	jks.
Key file password	slpassword.
"Get key file aliases" button	Click on the button to refresh the list of aliases.
Certificate alias to import	servicelink.



Step 4 Click **OK**.

Step 5 Click **Save directly to the master configuration**.

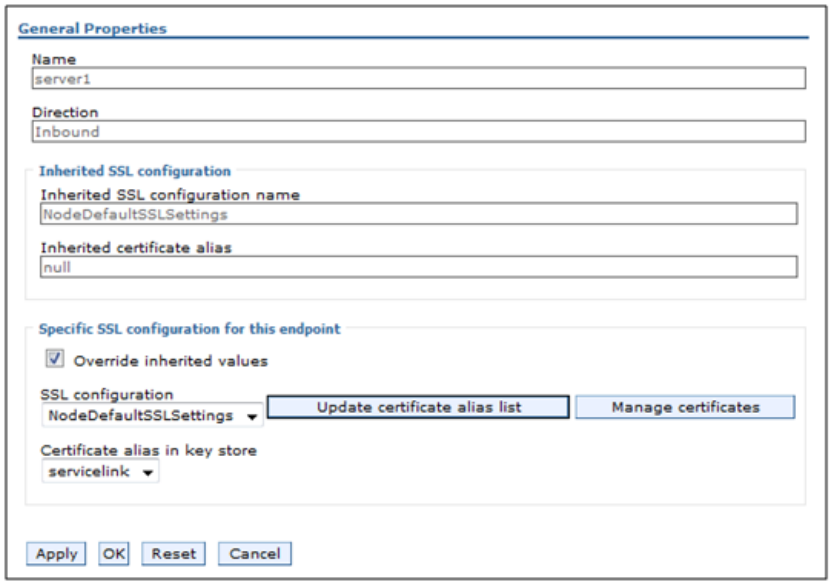
Step 6 Verify that the "servicelink" certificate was imported correctly:



Step 7 On the breadcrumb at the top of the current page, click on the name of your WebSphere server. For example, in the following screenshot, you would click on the "server1" link in the breadcrumb:

Step 8 Enter the following values:

Field	Value
Checkbox for "Override inherited values"	Select the checkbox.
SSL configuration	NodeDefaultSSLSettings.
"Update certificate alias list" button	Click on the button to refresh the list of aliases.
Certificate alias in key store	servicelink.



Step 9 Click **OK**.

Step 10 Click **Save directly to the master configuration**.

Step 11 Restart the WebSphere server where Service Link is deployed.

Step 12 Look in the log file "SystemOut.log" for messages similar to the followings, to ensure that the WebSphere server has started up in secure port (i.e. port 9443):

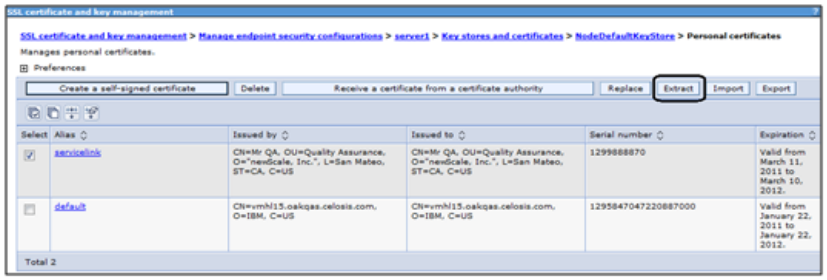
```
TCPC0001I: TCP Channel TCP_4 is listening on host *  (IPv4) port 9443.
CHFW0019I: The Transport Channel Service has started chain WCInboundDefaultSecure.
```

Your Service Link service is now SSL-enabled, and is using the "servicelink" certificate that you imported from file "slkeystore.jks".

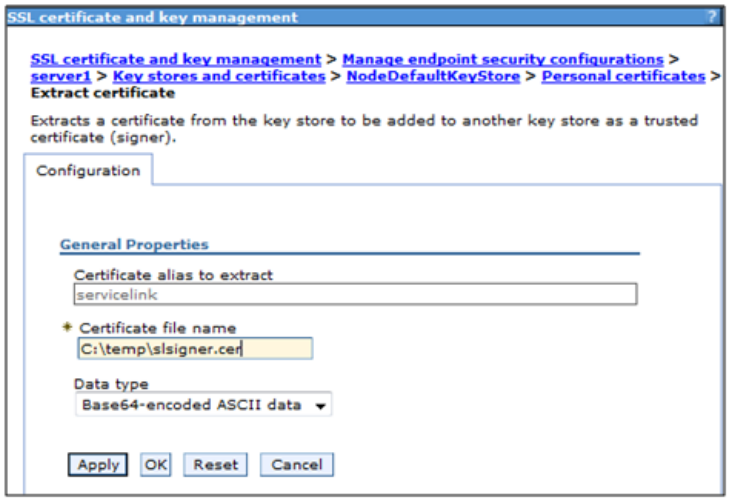
Step 13 If you decide to disable the non-secure port for the Service Link service, send file "slsigner.cer" (that you created at the beginning of this chapter) to the system administrator who manages the external system. That file contains the signer certificate for the "servicelink" certificate. It must be imported into the truststore of the external system, so that the external system can establish a trusted handshake with the Service Link service during SSL connection. In addition, the external system needs to connect to the **https** URL of the Service Link application. For example, previously, the Service Link URL may look like "http://<*servername*>:9080/ IntegrationServer/ ishttplistener/<*agent_name*>". The URL must now be changed to "https://<*servername*>:9443/IntegrationServer/ishttplistener/<*agent_name*>".

Step 14 If you have not created the file "slsigner.cer", you can do so now, by performing the following procedure:

a. Navigate back to the **Key stores and certificates > NodeDefaultKeyStore > Personal certificates** page.



b. Select the checkbox in front of the “servicelink” alias, then click the **Extract** button.



c. Enter the following values:

Field	Value
Certificate alias to extract	servicelink
Certificate file name	*<enter a value such as C:\temp\slsigner.cer>*
Data type	Base64-encoded ASCII data

d. Click **OK**.

For a clustered WebSphere environment only

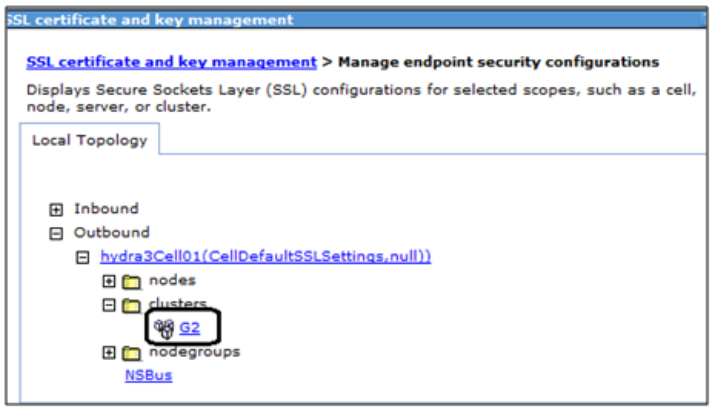
If you decide to disable the non-secure port for the Service Link service, then you must also import the signer certificate into the *Java Trusted Certificate Authority Keystore* of the Request Center services. This is because Service Link is running on a separate WebSphere server that does not belong to the cluster. (Only Request Center and the Business Engine can be installed on the cluster.) Request Center acts as a “client” that connects to the Service Link service at runtime. Complete the following procedure to import the signer certificate into the truststore for Request Center:

Step 1 Log on to the WebSphere Administration Console, and navigate to **Security > SSL certificate and key management**.

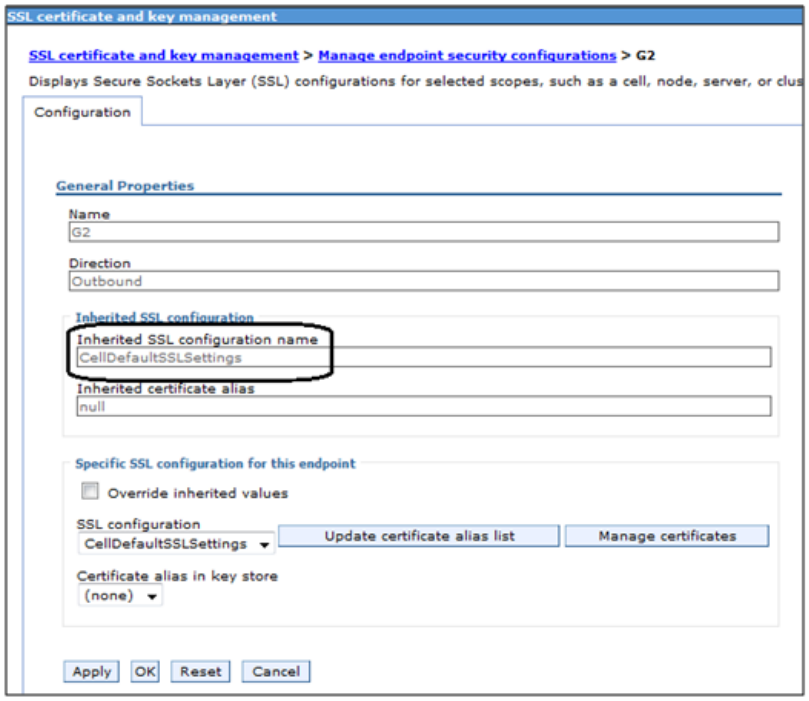
Step 2 Click **Manage endpoint security configurations**.

Step 3 Expand **Outbound > *<cell_name>* > clusters > *<cluster_name>***, where *<cluster_name>* is the WebSphere cluster on which Request Center application is deployed.

The following screenshot and the rest of the screenshots in this section are only examples. Your WebSphere environment will look different with regards to <cell_name> and <cluster_name>.



Step 4 Click on the ***<cluster_name>*** link to open its configuration page. Find out what is displayed in the "Inherited SSL configuration name" field. For example, in the screenshot below, the "Inherited SSL configuration name" field is set to the value "CellDefaultSSLSettings".



Step 5 Under the Related Items section on the right-hand side, click on **SSL configuration**, then click on **CellDefaultSSLSettings**.

Step 6 Check the value in the field "Trust store name". For example, the value is set to "CellDefaultTrustStore".

Step 7 Click **Key stores and certificates** under the Related Items on the right-hand side.

Step 8 Click on **CellDefaultTrustStore**.

Step 9 Click **Signer certificates** on the right-hand side.

Step 10 Click the **Add** button.

Step 11 Enter the following values, then click **OK**:

Field	Value
Alias	servicelink
File name	C:\slsigner.cer
Data type	Base64-encoded ASCII data

Step 12 Click **Save directly to the master configuration**.

Step 13 Modify file "**newscale.properties**" under the directory "RequestCenter.ear\ config\" as follows:

Search for the following parameter:

```
isee.base.url=http://<hostname>:9080
```

and change to:

```
isee.base.url=https://<hostname>:9443
```

Step 14 Repeat Step 13 for every node in the WebSphere cluster where Request Center is deployed.

Step 15 Restart the WebSphere cluster for Request Center.

Step 16 To avoid Step 1 above, you may decide to turn on both non-secure port and secure ports for the Service Link service. This way the Request Center application (running in the WebSphere cluster) can still connect to Service Link using the non-secure URL (http://<*hostname*>:9080). But you may want to consider taking some measures (such as a firewall system) to block access to the non-secure port from all external systems.

Configuring SSL for Service Link Outbound Documents

Overview

When a Service Link agent uses the http/ws adapter to send an outbound message to an external system, it acts as a client that posts http requests or web services request to the external web server. If the external web server is SSL-enabled, Service Link may require some configuration in order to establish a secure connection with that web server.

- The Outbound URL of the Service Link agent must point to the https address with the secured port number of the external web server.
- To establish a trusted handshake via SSL, the client (that is, the Service Link service) must have a valid signer certificate (the public key certificate) that can validate the digital certificate of the external web server. If the certificate of the external web server is not signed by a well-known Certificate Authority (CA) such as VeriSign, then most likely during the SSL handshake, Service

Link will not be able to validate the external web server's certificate, and the connection will fail. If this is the case, the signer certificate must be imported into the *Trusted Certificate Authority Keystore* used by the Service Link service.

Note If Service Link is connecting to multiple SSL-enabled web servers, it may be necessary to import multiple signer certificates, one for each external web server.

Service Link, as a client, does not support Client Certificate Authentication during SSL handshake.

The following sections describe the configuration procedure in more detail.

Outbound URL

Step 1 Log on to Request Center as a user who can access Service Link.

Step 2 Navigate to the Service Link module and select the **Manage Integrations** tab.

Step 3 Select the agent that you want to configure.

Step 4 Open the Outbound Properties page of the agent.

Step 5 In the **HttpOutboundAdapter.RoutingURL** field, enter the https address with the secured port number, for example, https://192.168.21.202:8444/HTTPSimulator/.

Step 6 Set the value for the **HttpOutboundAdapter.AcceptUntrustedURL** field to **false** to ensure a secure connection.

Step 7 Click **Save**.

Importing the Signer Certificate to a Trusted CA Keystore

The instructions for importing the signer certificate depend on the application server ("JBoss 4.2.3", "WebLogic 10.3", or "WebSphere 7") that Service Link is running on. Before following the application server-specific instructions, you must complete the following step:

- Get the signer certificate of the external web server in a file. To do this, you can contact the system administrator who manages the external web server, and ask him/her to export the signer certificate (the public key) of the digital certificate used to secure that web server. The signer certificate must be exported in the "**Base64-encoded ASCII**" format. The following is an example of what a Base64-encoded signer certificate looks like:

```
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCBE17w1cwDQYJKoZIhvcNAQEEBQAwZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNB
MRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG51d1NjYWxlMQswCQYDVQQLEwJRQTEVMBMG
A1UEAxMMS2hhbmcgTmd1eWVuMB4XDTExMDMxMjE5MDI0N1oXDTIxMDMwOTE5MDI0N1owZTELMAkG
A1UEBhMCVVMxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG51d1Nj
```

```
YWxlMQswCQYDVQQLEwJRQTEVMBMGA1UEAxMMS2hhbmcgTmd1eWVuMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDhTxg2RwarD6Wn4iqYeOOk3ykfXzZiDArf/X63omXquTmN0Up+mg6oJmPAfqJA
l7k4+Dn7dfVtAc4h8qra7PBeBU48zrzRqZd6VAK07rz++CilQto64mHXYVomb5vWPGeKA41j9vlv
ENj/tE/6++IqbwnxAqeZtY3EvEM7dcCWDwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAAaqCnfEAovy
Uf2S+oAXYDo5N387a035APsz5iiUM5oiKR/KW3oRz/v0P0I/o3n312kDIJ01111pl6qpZRtPEsr1
b00Tu1cXfPmizEtz0ole606qDS+DzkS1+YYz2mLL2Zq40d1EPsMolyqyUmyq3GHaEnuhWemcv2aA
wGFgbQYd
-----END CERTIFICATE-----
```

Note If the signer of the external web server's certificate is a well-known Certificate Authority like VeriSign or Thawte, then most likely, you can skip this step since Sun JDK already recognizes many well-known CA signers. On WebSphere, you still need to complete this step because the WebSphere truststore does not contain third-party Certificate Authority signers.

JBoss 4.2.3

Perform the following steps as the "administrator" user of the Service Link machine:

Step 1 Copy the signer certificate file (of the external system) to a temporary directory on the Service Link machine. For example, if the signer certificate file is called "extws.cer", then copy this file to "C:\temp\extws.cer" on the Service Link machine.

Step 2 On the Service Link machine, locate the file "**cacerts**" in the directory "<*JAVA_HOME*>\jre\lib\security", where <*JAVA_HOME*> is the root directory of the Sun JDK 6 installation. This file is the *Trusted CA Keystore* that comes with the Sun JDK 6 installation.

Note Verify that <JAVA_HOME> is the Java directory used by your JBoss application server. Look for the JAVA_HOME setting inside the file "setEnv.cmd", located under the "<APP_HOME>\bin" directory. For example: *set JAVA_HOME=C:\jdk1.6.0_23*.

Step 3 Import the signer certificate into the "cacerts" keystore by executing the following commands in a Command Prompt window:

```
cd <JAVA_HOME>\jre\lib\security
<JAVA_HOME>\bin\keytool -import -trustcacerts -alias extws –noprompt  -file
C:\temp\extws.cer -keystore cacerts -storepass changeit
```

Note In the command above, it is assumed that the password for the "cacerts" keystore file is still the default value of "changeit". Replace this with the correct value for the password in your environment. For the –alias parameter, you can replace the value "extws" with an appropriate alias you plan to use for this signer certificate. If you import multiple signer certificates, make sure to assign a unique alias name to each signer certificate.

Step 4 Restart the Service Link service.

WebLogic 10.3

Perform the following steps as the "root" user (if on UNIX/Linux) or the "administrator" user (if on Windows) of the WebLogic machine:

Step 1 Copy the signer certificate file (of the external system) to a temporary directory on the WebLogic machine where Service Link service is running. For example, if the signer certificate file is called "extws.cer", then copy this file to "/tmp/extws.cer" on the Service Link machine.

In a clustered WebLogic environment, Service Link must be deployed in a WebLogic server that does not belong to the cluster. So, make sure you find the correct WebLogic server for Service Link.

Step 2 On the Service Link machine, locate file "**cacerts**" in the directory "<*JAVA_HOME*>/jre/lib/security", where <*JAVA_HOME*> is the root directory of the Sun JDK 6 installation. This file is the *Trusted CA Keystore* that comes with the Sun JDK 6 installation.

Make sure that <JAVA_HOME> is the correct Java directory used by your WebLogic application server. To verify this, look for the JAVA_HOME setting inside file "commEnv.sh" (on Windows, look for "commEnv.cmd"), located under the "<WL_HOME>/common/bin" directory. For example: JAVA_HOME="/opt/jdk1.6.0_23".

Step 3 Import the signer certificate into the "cacerts" keystore by executing the following commands in a Command Prompt window:

```
cd <JAVA_HOME>/jre/lib/security
<JAVA_HOME>/bin/keytool -import -trustcacerts -alias extws –noprompt  -file /tmp/extws.cer
-keystore cacerts -storepass changeit
```

Note In the command above, it is assumed that the password for the "cacerts" keystore file is still the default value of "changeit". Replace this with the correct value for the password in your environment. For the –alias parameter, you can replace the value "extws" with an appropriate alias you plan to use for this signer certificate. If you import multiple signer certificates, make sure to assign a unique alias name to each signer certificate.

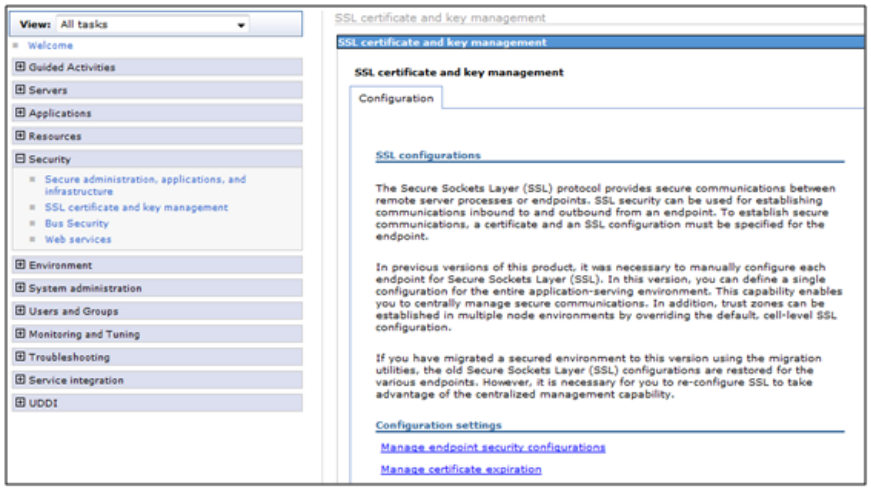
Step 4 Restart the WebLogic server where Service Link is deployed.

WebSphere 7

Perform the following steps as a user who can access the WebSphere Administration Console:

Step 1 Copy the signer certificate file (of the external system) to a temporary directory on the machine where the WebSphere Administration Server is running. For example, if the signer certificate file is called "extws.cer", then copy this file to "C:\temp\extws.cer" on the WebSphere machine.

Step 2 Log on to the WebSphere Administration Console, and navigate to **Security > SSL certificate and key management**.

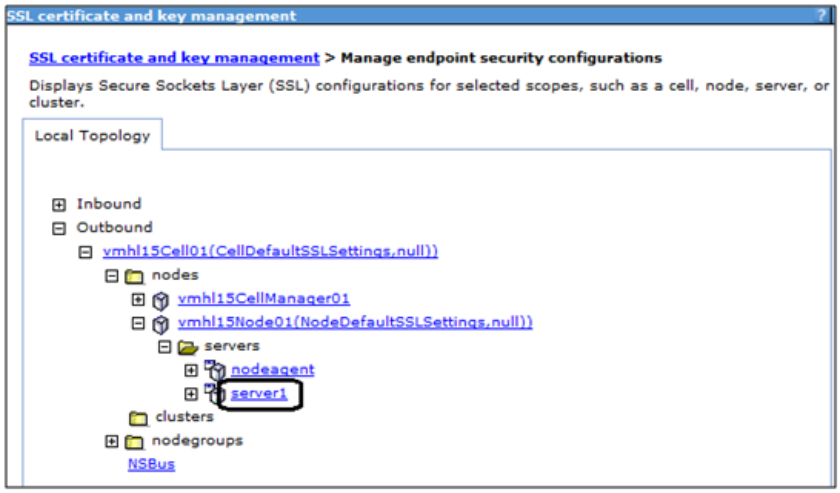


Step 3 Click **Manage endpoint security configurations**.

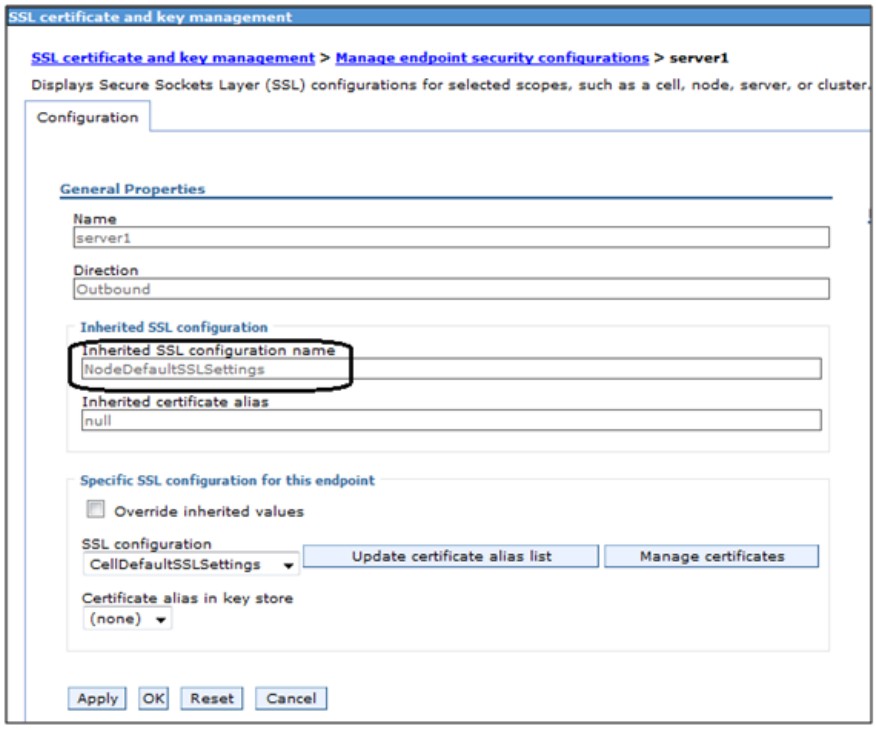
Step 4 Expand **Outbound > *<cell_name>* > nodes > *<node_name>* > servers > *<SL_server>***, where *<SL_server>* is the WebSphere server on which Service Link is deployed.

In a clustered WebSphere environment, Service Link must be deployed in a WebSphere server that does not belong to the Cluster. So, make sure you locate the correct WebSphere server for Service Link.

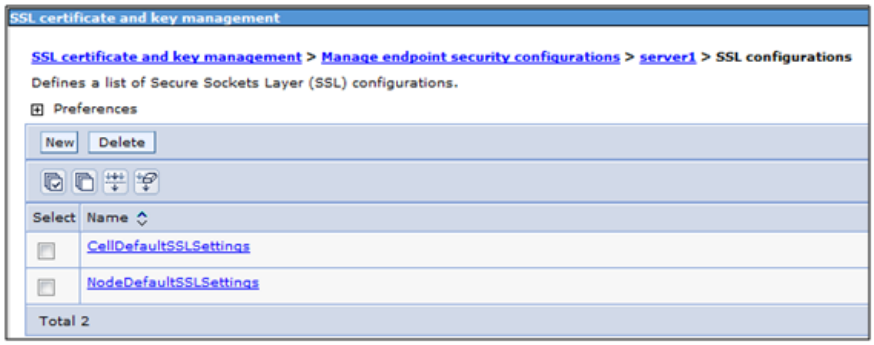
All screenshots in this section show sample values for <cell_name>, <node_name> and <SL_server>. Replace these with values appropriate to your WebSphere environment.



Step 5 Click on the ***<SL_server>*** link to open its configuration page. Find out what is displayed in the "Inherited SSL configuration name" field. For example, in the screenshot below, the "Inherited SSL configuration name" field is set to the value "NodeDefaultSSLSettings".

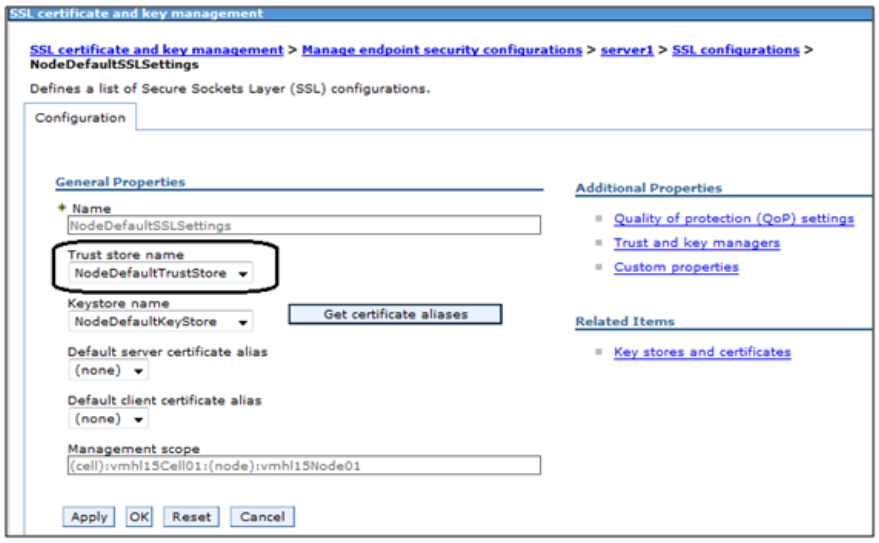


Step 6 Under the Related Items section on the right-hand side, click on **SSL configuration**, then click on **NodeDefaultSSLSettings**.



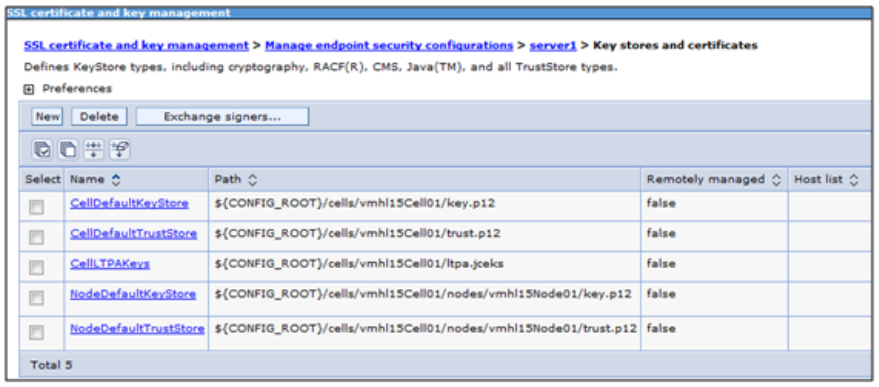
Step 7 On the NodeDefaultSSLSettings page, set the following values, then click **OK**:

Field	Value
Trust store name	NodeDefaultTrustStore
Keystore name	NodeDefaultKeyStore

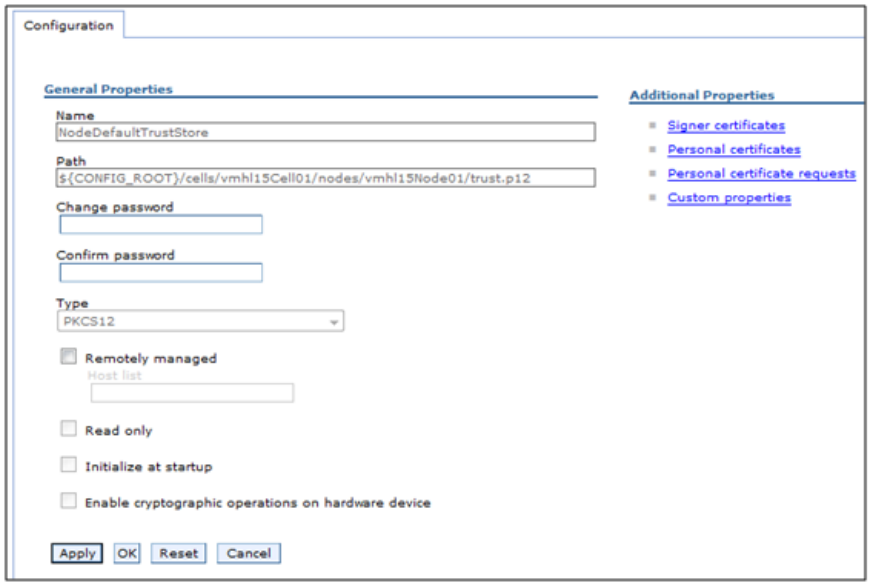


Step 8 Click **Save directly to the master configuration**.

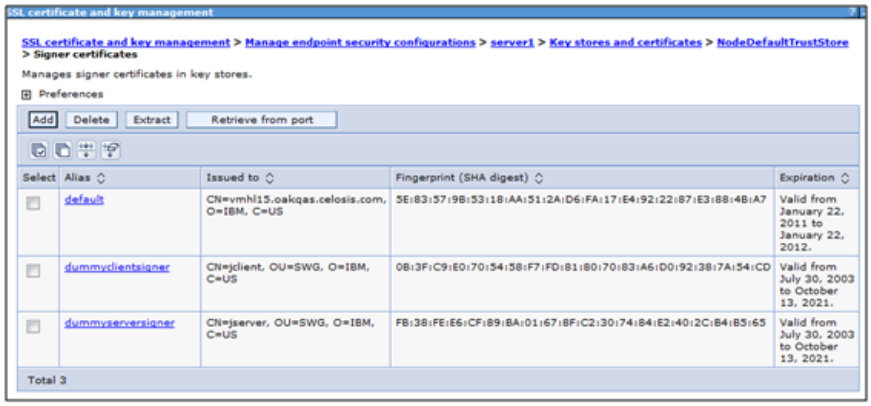
Step 9 Re-open the "NodeDefaultSSLSettings" page again (as seen the screenshot above), and click **Key stores and certificates** under the Related Items section on the right-hand side.



Step 10 Click on **NodeDefaultTrustStore**.



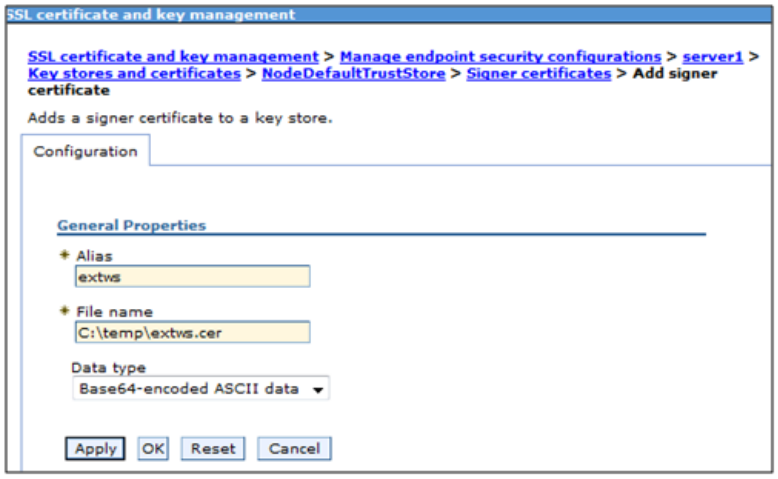
Step 11 Under the Additional Properties section on the right-hand side, click on **Signer certificates**.



Step 12 Click the **Add** button.

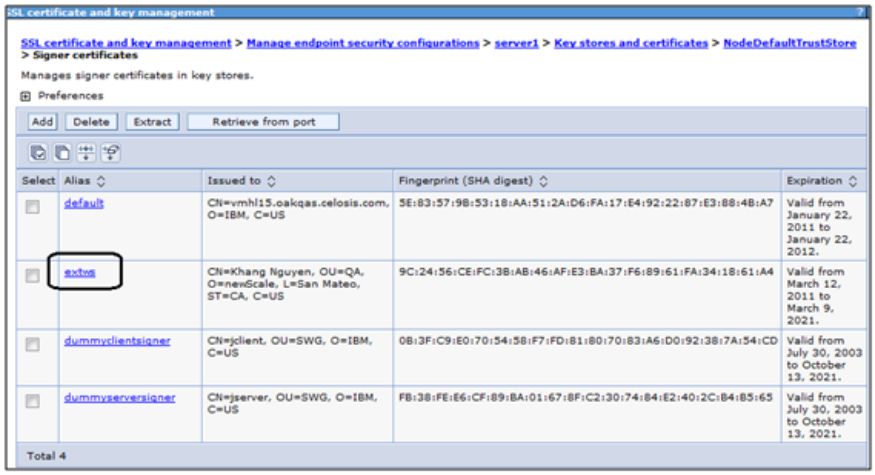
Step 13 Enter the following values, then click **OK**:

Field	Value
Alias	A value for the signer certificate (that is, “extws”).
File name	The path to the signer certificate file (that is, “C:\temp\extws.cer”).
Data type	Select the value “Base64-encoded ASCII data” in the dropdown.



Step 14 Click **Save directly to the master configuration**.

Step 15 Review the newly added certificate (in this example, “extws”) to verify that the information is correct.



Step 16 Restart the WebSphere server where Service Link is deployed.

Troubleshooting

This section provides information about WebSphere tracing, how to limit outbound email and to control email generation. This section also includes information about contacting Cisco with support questions and methods for keeping track of your system environment and error information.

Commonly Monitored Traces and WebSphere Tracing

Commonly Monitored Traces

For Database Interactions

com.newscale.bfw.udkernel.udsql.UdSqlBean

com.newscale.bfw.udkernel.util.UdKernelUtil

For LDAP Interactions

com.newscale.bfw.ldap.jldap.JLDAPApi

For Clustering Issues

com.opensymphony.oscache.plugins.clustersupport.AbstractBroadcastingListener

com.opensymphony.oscache.plugins.clustersupport.JavaGroupsBroadcastingListener

Enabling WebSphere Tracing

Complete the following steps to enable WebSphere tracing on your system:

Step 1 Navigate to **Logging and Tracing > [*Yourserver*] > Configuration**.

Step 2 Click on **Modify**.

Step 3 From the items in the tree displayed, expand the **Servlet_Engine** node.

Step 4 Turn **on** debug for:

```
com.ibm.ws.webcontainer.srp.ServletRequestProcessor
com.ibm.ws.webcontainer.webapp.WebApp
```

Step 5 Click **Apply** and then **Close**.

Step 6 Click **Apply** again.

Step 7 Save the configuration change to Master configuration and restart Webapp.

Limiting Outbound Email

You may want to limit outbound email during service design testing or in non-production environments.

By limiting outbound email capabilities, you can limit or prevent the sending of email to actual performers or customers on whose behalf services are ordered.

Ways to Limit Outbound Email

Changing all email templates to have “fake addresses” in a development environment is not really an option. Firstly, it would be very time consuming. More important, much of the testing is invalidated when the template addresses are changed back—you would still need to ascertain that the correct people are receiving the appropriate emails.

If templates use only namespace variables and users in the non-production environment are refreshed via directory integration, you could change the LDAP mapping to give everyone the same email address or a similar fake address, for example:

User@<company>.com, or

reqcentertest@<company>.com

by using a mapping similar to:

```
expr:#cn#=(cannotmatch)?(neverthis):requestcenter@<company>.com
```

However, this approach also does not allow you to adequately test the accuracy of email delivery.

A more robust solution is to use a dedicated SMTP (email) server for the development instance and any other instances where emails should not be distributed outside the box. You can set up an SMTP server that routes ALL emails (whether fake or correct) to a standard mailbox (for example, rctestmailbox@company.com) for the development and test servers. This way, you don't have to change Request Center configuration in any way, and emails could be tested very easily. The project team just needs to be able to open that test mailbox.

This requires the customer be able to configure a separate test SMTP server that overrides the recipients to always forward to the test email box. Production would need to point to the production SMTP server, of course.

If you use any of these techniques, add the To/Cc addressees in the HTML body of the email templates surrounded by <!-- Comment --> tags so that testers may validate the namespace expression and other logic for these fields.

Controlling Email Generation

Request Center controls the outgoing email envelope and defaults to sending a single message to multiple recipients. The multiple-recipient messages are sent to the same SMTP server.

The alternative is to send single recipient emails has a minimal negative effect on CPU and network bandwidth usage. This is enabled via a setting in the be.properties file:

```
Email.One.Per.Recipient=true
```

Use this setting only to avoid SMTP server problems whereby the entire message is rejected if one recipient is invalid.

SMTP connections are tried Email.ServerDownCount=10 times and then paused for Email.RescheduleOffset (msec).

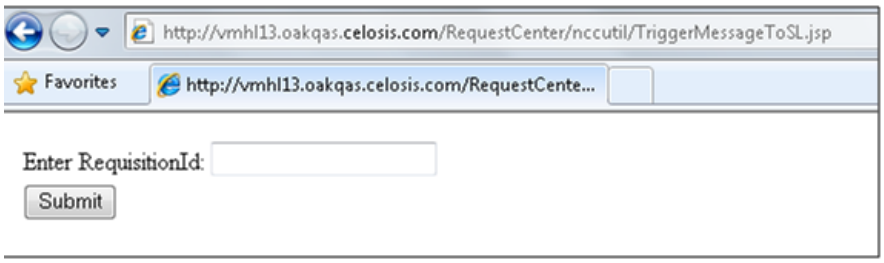
Full mailboxes, bounces or other delivery problems are retried based on the Email.RetryCount=4 setting.

Recreating Missing Service Link Messages

In the rare occasion of extended outage or incorrect configurations of the Service Link application, external tasks might not have corresponding outbound messages created in Service Link.

Once the underlying issue is resolved in Service Link and the application is up and running, the problem external tasks can be republished to Service Link to allow the outbound messages to be created and the delivery plan to continue. The republish utility can be accessed at:

http:// <host>:<port>//RequestCenter/nccutil/TriggerMessageToSL.jsp



Enter the Requisition ID for the requests which have one or more missing outbound Service Link messages. All authorization and delivery tasks associated with the requisition will be evaluated and only those tasks that require republishing will be processed for outbound message creation.

Environment/Platform Overview

It is useful to document the systems in your environment by using a matrix like the one provided in the "Sample Environment Matrix" section on page 5-81.

Cisco publishes a support matrix detailing the software on which each version of Service Portal is certified. The Cisco Technical Assistance Center (TAC) will always have the most current version of this matrix, adjusted for point releases and Service Packs.

When to Call the Cisco Technical Assistance Center (TAC)

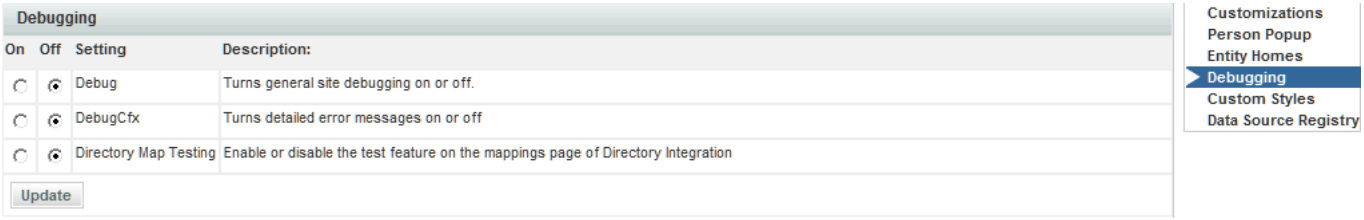
It is a good idea to inform the Cisco Technical Assistance Center (TAC) before performing any system maintenance tasks that may affect:

- server operating system patches/upgrades
- database server patches/upgrades
- Service Portal application server patches or upgrades – Validate the update is supported by Cisco first!
- LDAP Directory tree structure changes
- Single Sign-On system upgrades

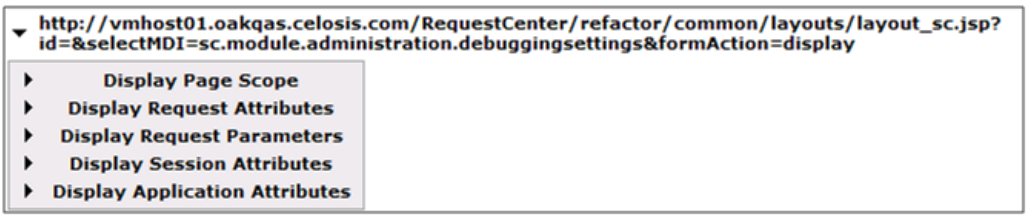
Collecting Troubleshooting Information

Site Debugging

If an “Our Apologies” exception occurs, you may turn on Site Debugging via the Debugging option of Administration module Settings.



Debugging adds the URL of the current page at the bottom of the page. Clicking on the URL provides links to additional information which may be helpful to Cisco support personnel.



When you are finished, don’t forget to turn debugging off, as it may confuse end-users. It also adversely affects performance.

The application log is a key troubleshooting mechanism. Looking in this log for “Exception” (from the bottom up) often reveals the applicable error message.

In a clustered environment, it is often useful to browse the log files from all the machines in the cluster for the period in question.

Service Link Log Files

Logs for the Service Link server show the details of all Service Link transactions for that day. It is often useful to correlate that file to the Request Center server log when troubleshooting issues that have to do with the interaction between the Business Engine and Service Link.

Performance

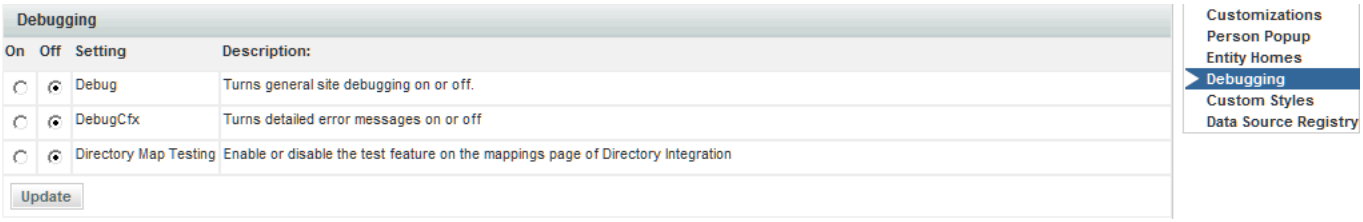
Gather performance information from the log and native_stderr.log files.

Service Design and Platform Dependence

Problems that arise during service design may be related to incorrect service configuration. Problems that occur only in a production environment may be data-dependent or platform-dependent. In some case, the Cisco Technical Assistance Center (TAC) may ask for a dump of the database to be sent, where it can be installed in a testing lab that can closely emulate the environment where the error occurred. Customers should have logins and credentials that allow them to upload the database to the Cisco support site for investigation.

"Our Apologies" Exceptions

Turn on Site Debugging via the Debugging option of Administration module Settings.



Debugging adds the URL of the current page at the bottom of the page. Clicking on the URL provides links to additional information. When you are finished, don't forget to turn debugging off, as it may confuse end-users. It also adversely affects performance.

The application log is a key troubleshooting mechanism. Looking in this log for "Exception" (from the bottom up) often reveals the applicable error message.

In a clustered environment, it is often useful to browse the log files from all the machines in the cluster for the period in question.

Service Link

Logs for the Service Link server show the details of all the transactions for that day. It is often useful to correlate that file to the Request Center log when troubleshooting issues that have to do with the interaction between the Business Engine and Service Link.

Performance

Gather performance information from the log and native_stderr.log files.

How to Reach Product Support

Contact the Cisco Technical Assistance Center (TAC)

- For Solutions
  - Get access to the documentation library
  - Learn about upgrades and patches
  - Learn answers to Common Issues
- About Cases
  - Log new cases
  - Check status of cases
  - Read/Update case investigation comments
  - Attach logs/files

Errors

This section provides information regarding critical error conditions. The information is presented according to individual error messages, and includes the following information for each condition:

- Error Condition
- Error Message
- Probable Cause
- Location of Error Log
- Recommended resolution

Error Log Locations

Error logs for Service Portal and its related components are in the following locations:

Component	Error Log Location
Application Server	
WebLogic	<BEA_HOME>/user_projects/domains/<domain>/servers/<server>/logs/<server>.log
WebSphere	<WAS_HOME>/profiles/<profilename>/logs/server1/SystemOut.log
JBoss	<JBOSS_HOME>/server/RequestCenter/log/server.log <JBOSS_HOME>/server/ServiceLink/log/server.log
ColdFusion Services	RequestCenter.war/WEB-INF/cfusion/logs

Error Conditions and Error Codes

The following error conditions are presented according to the error condition or its related error message.

Some error conditions cause the same system behavior although the error itself may stem from one of several different error conditions within the system. For example, if you cannot connect to the LDAP server, several error conditions below may apply. It is important to match the error message to the error you are experiencing.

All errors are written to the Request Center server log file, whose behavior and location are described earlier.

Request Center is unable to perform Asynchronous Submit/Authorization

Error Condition	Request Center is not able to instantiate a task plan asynchronously, after the request submission and/or the last authorization/review in the service.
Error Message	Requisition *xxx* [Task "*<name of task here>*"]: We're sorry but his approval/review cannot be completed at this time because the Request Center queue that processes these tasks is temporarily unavailable. Please try again later or contact your Request Center system administrator.
Resolution	Verify that the JMS queue which serves the asynchronous submit/last authorization process is available for receiving messages.

Application Server Loses Connection to the Database

Error Condition	Application server lost the connection to the database.
Error Message	ERROR [com.celosis.logger.FatalerrorChannel] (8000)SQLException in getConnection:Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver]Error establishing socket. Connection refused: connect); - nested throwable: (org.jboss.resource.JBossResourceException: Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver]Error establishing socket. Connection refused: connect)) Code: 0 State: null.
Resolution	Check the RequestCenter database. If the RequestCenter database is not running, start it. Once the database is up, the application server will automatically connect to it.

Application Fails to Authenticate with the Database

Error Condition	Application failed to authenticate with the database using the configured username and password.

Error Message	ERROR [com.newscale.bfw.udkernel.util.UdPersistenceManagerImpl] Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver][SQLServer]Login failed for user 'RCUser'.); - nested throwable: (org.jboss.resource.JBossResourceException: Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver][SQLServer]Login failed for user 'RCUser'.))
Resolution	Verify that the user-name and password parameters are configured correctly in the following configuration file: <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy\requestcenter-ds.xml. If you modify this configuration file, you must restart the Request Center and Service Link applications.

Failure to Connect to the LDAP Server – Incorrect Port

Error Code	LDAPException 91.
Error Condition	Cannot connect to the LDAP server. Most likely the LDAP server is down or you have an incorrect port number.
Error Message	ERROR [com.newscale.bfw.ldap.jldap.JLDAPNonSSLConnection] LDAPException in NON-SSL Connection: LDAPException: Unable to connect to server <hostname>:<port> (91) Connect Error java.net.ConnectException: Connection refused: connect
Resolution	Check to see if the LDAP server is running. If not, start the LDAP server. Check the LDAP System Connection Parameters on **Administration > Directories**. Verify that the Connection Port value is correct. You do not need to restart the Request Center application.

Failure to Connect to the LDAP Server – Incorrect Hostname

Error Code	LDAPException 91
Error Condition	Cannot connect to the LDAP server. Most likely incorrect hostname.
Error Message	ERROR [com.newscale.bfw.ldap.jldap.JLDAPNonSSLConnection] LDAPException in NON-SSL Connection: LDAPException: Unable to connect to server <hostname>:<port> (91) Connect Error java.net.UnknownHostException: <hostname>
Resolution	Check the LDAP System Connection Parameters on **Administration > Directories**. Verify that the LDAP Host value is correct.

Failure to Connect to the LDAP Server – LDAPException 32

Error Code	LDAPException 32
Error Condition	Cannot connect to the LDAP server. Most likely incorrect authenticated user id.
Error Message	ERROR [com.newscale.bfw.ldap.jldap.JLDAPSimpleAuth] LDAPException in Simple Auth: LDAPException: No Such Object (32) No Such Object LDAPException: Matched DN:
Resolution	Check the LDAP System Authentication Parameters on **Administration > Directories**. Verify that the BindDN value is correct.

Failure to Connect to the LDAP Server – LDAPException 49

Error Code	LDAPException 49
Error Condition	Cannot connect to the LDAP server. Most likely incorrect authenticated password.
Error Message	ERROR [com.newscale.bfw.ldap.jldap.JLDAPSimpleAuth] LDAPException in Simple Auth: LDAPException: Invalid Credentials (49) Invalid Credentials
Resolution	Check the LDAP System Authentication Parameters on **Administration > Directories**. The Password field is encrypted and thus you can not verify its existing value. Just enter a correct value for the Password, and click **Update**.

Failure to Connect to the LDAP Server

Error Condition	Cannot connect to the LDAP server.
Error Message	FATAL [LDAPBase] LDAP instance cannot be created netscape.ldap.LDAPException: no host for connection (89)
Resolution	Check to see if the LDAP server is running. If not, start the LDAP server. You do not need to restart the Request Center application server.

Failure to Connect to the LDAP Server

Error Condition	Cannot connect to the LDAP server.
Error Message	ERROR [com.newscale.bfw.ldap.LDAPQuery] LDAP netscape.ldap.LDAPException: failed to connect to server ldap://<hostname>:<port> (91)
Resolution	Check to see if the LDAP server is running. If not, start the LDAP server. You do not need to restart the Request Center application server.

Failure to Authenticate with the LDAP Server

Error Condition	Fail to authenticate with the LDAP server.
Error Message	ERROR [com.newscale.comps.user.dao.LDAPUserDataSource] Single Person search failure, exception thrown: null com.newscale.bfw.dataaccess.DataAccessException
Resolution	Check the Data Source Configuration on the **Administration > Directories** page. Verify the following parameters and correct if necessary: • BindDN • Password • User BaseDN You do not need to restart the Request Center application server.

Attribute Name is Mapped Incorrectly

Error Condition	One of the required attributes is incorrectly mapped. Thus the person cannot be found in the LDAP server.
Error Message	ERROR [com.newscale.bfw.ldap.LDAPQuery] LDAP java.lang.RuntimeException: Required LDAP attribute <attribute_name> is missing from the LDAP system.
Resolution	Correct the attribute name in the Directory Data Mapping. You do not need to restart the Request Center application server.

User Base DN in LDAP Server is Missing

Error Code	LDAPException 32
Error Condition	Cannot find the User Base DN in LDAP server.
Error Message	ERROR [com.newscale.bfw.ldap.jldap.JLDAPApi] Referral Exception during Result Set iteration: LDAPException: No Such Object (32) No Such Object
Resolution	Check the LDAP System Authentication Parameters on the **Administration > Directories** page. Verify that the LDAP User BaseDN value is correct.

Failure to Connect to the LDAP Server in SSL Mode

Error Condition	(For SSL connection only) Cannot connect to the LDAP Server in SSL mode, because the SSL certificate keystore has not been created.

Error Message	DEBUG [com.newscale.bfw.ldap.util.LDAPConfUtil] The LDAP configuration file "/C:/newScale/jboss-4.2.3.GA/server/RequestCenter/deploy/RequestCenter.ear/config/<LDAP_System>_TrustCertDB.keystore" does not exist.
Resolution	Add the appropriate server certificate for the LDAP System on the **Administration > Directories** page.

Failure to Connect to the LDAP Server in SSL Mode

Error Condition	(For SSL connection only) Cannot connect to the LDAP Server in SSL mode, because the server certificate in the keystore is NOT correct.
Error Message	ERROR [com.newscale.bfw.ldap.jldap.JLDAPSimpleAuth] LDAPException in Simple Auth: LDAPException: I/O Exception on host <hostname>, port <port number> (91) Connect Error javax.net.ssl.SSLException: Connection has been shutdown: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate found
Resolution	The certificate keystore may already exist, but does not contain the correct certificate used with this LDAP Server. Obtain the correct certificate used for the LDAP server, and add it for the same LDAP System on the **Administration > Site Configuration** page.

"Common OU for new users" Configuration Value is Missing

Error Condition	The "Common OU for new users" configuration value is either missing or does not exist in RequestCenter database.
Error Message	ERROR [com.newscale.comps.user.dao.LDAPUserDataSource] Error getting Person from Ldap java.lang.NullPointerException at com.newscale.comps.user.dao.LDAPUserDataSource.transferOrgUnitVOToBO(LDAPUserDataSource.java:676)
Resolution	Check the LDAP System Lookup Configuration on the **Administration > Site Configuration** page. Select a correct value for the **"**Common OU for new users**"** field.

User cannot be Found in the LDAP Server

Error Condition	The <attribute_name> is incorrectly mapped. Thus, the person cannot be found in the LDAP server.
Error Message	WARN [com.newscale.bfw.ldap.jldap.JLDAPApi] Required LDAP attribute <attribute_name> is missing from the LDAP system, for DN : …
Resolution	Correct the attribute name on the Directory Mapping page, for the appropriate LDAP System.

Failure to Connect to a Referral LDAP System

Error Condition	Cannot connect to one of the Referral LDAP Systems. (The config flag SkipErrorOnLDAPSystem=true; thus, Request Center system ignores this error.)
Error Message	WARN [com.newscale.bfw.ldap.jldap.JLDAPApi] Referral Exception during Result Set iteration: LDAPReferralException: Search result reference received, and referral following is off (10)
Resolution	Check to see if the Referral LDAP server is running. Verify the Authentication and Connection for the Referral LDAP System.

Failure to Connect to the External Data Dictionary Database

Error Condition	Cannot connect to the External Data Dictionary Database.
Error Message	ERROR [STDERR] SQLException while attempting to connect: java.sql.SQLException: [Macromedia][SQLServer JDBC Driver]Error establishing socket. Connection refused: connect.
Resolution	Check the External Data Dictionary database. If the External Data Dictionary database is not running, start it. You do not need to restart the Request Center application.

Request Center Fails to Authenticate with the External Data Dictionary DB

Error Condition	Request Center fails to authenticate with the External Data Dictionary database using the configured username and password.
Error Message	ERROR [FatalerrorChannel] (1523)Fatal error happened java.lang.Exception: GetTables can not connect to <username>@RequestCenter GetTables can not connect to <username>@RequestCenter [newScale][SQLServer JDBC Driver][SQLServer]Login failed for user '<username>'. Connect String:jdbc:newscale:sqlserver://<hostname>:1433;DatabaseName=<database_name>.
Resolution	Check the username and password parameters in the following configuration file: <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy\RCExtData-ds.xml. Each application server has its own version of the datasource RCExtData. Details for setting up external datasources are in the *Cisco Service Portal Installation Guide*. For JBoss/SQL Server: If you modify this configuration file, you must restart the Request Center application server.

Lost Connection to the Database

Error Condition	Lost the connection to the database.
Error Message	ERROR [com.celosis.logger.FatalerrorChannel] (8000)SQLException in getConnection: Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver]Error establishing socket. Connection refused: connect)
Resolution	Check the database. If the database is not running, start it. Once the database is up, the application server will automatically connect to it.

Business Engine Fails to Authenticate with Database

Error Condition	The Business Engine fails to authenticate with the database using the configured username and password.
Error Message	ERROR [com.celosis.logger.FatalerrorChannel] (8000)SQLException in getConnection: Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver][SQLServer]Login failed for user 'RCUser'.)
Resolution	Verify that the username and password parameters are configured correctly in the following comfit file: <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy\requestcenter-ds.xml. If you modify this configuration file, you must restart the Request Center application.

External Datasource Configuration Missing

Error Condition	Missing External Datasource configuration.
Error Message	ERROR [com.newscale.bfw.udkernel.database.UdContainerConnectionPool] Connection to external datasource cannot be established javax.naming.NameNotFoundException: <DataSource_Name> not bound
Resolution	• Navigate to <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy. • Make a copy of requestcenter-ds.xml. • Rename copied version to RcExtData-ds.xml. • Open RcExtData-ds.xml using a text editor. • Change <jndi-name> value to RcExtData. • Change all of the other connection parameters to match your External Data Dictionary database (host, database-name, user-name, password, etc...), • Save RcExtData-ds.xml. If you modify this configuration file, you must restart the application server. This is for JBoss only; refer to the *Cisco Service Portal Installation Guide* for information about other application servers.

Failure to Connect to the External Data Dictionary Database

Error Condition	Cannot connect to the External Data Dictionary Database.
Error Message	ERROR [com.newscale.bfw.udkernel.udsql.UdSqlBean] Message: [newScale][SQLServer JDBC Driver]Connection reset by peer: socket write error.
Resolution	Check the External Data Dictionary database. If the External Data Dictionary database is not running, start it. You do not need to restart the Request Center application.

Business Engine Fails to Authenticate with the External Data Dictionary DB

Error Condition	The Business Engine fails to authenticate with the External Data Dictionary database using the configured username and password.
Error Message	ERROR [com.newscale.bfw.udkernel.udsql.UdSqlBean] Message: Could not create connection; - nested throwable: (java.sql.SQLException: [newScale][SQLServer JDBC Driver][SQLServer]Login failed for user '<username>'.)
Resolution	Check the user-name and password parameters in the following configuration file: <APP_HOME>\jboss-4.2.3.GA\server\RequestCenter\deploy\RCExtData-ds.xml. You do not need to restart the Request Center application.

Integration Server Fails to Connect to the Database

Error Code	LogID=1877
Error Condition	Integration Server cannot connect to the database.
Error Message	Exception occurred: java.sql.SQLException: [newScale][SQLServer JDBC Driver]Error establishing socket. Connection refused: connect or Exception occurred: java.sql.SQLException: [newScale][SQLServer JDBC Driver]Error establishing socket. No route to host: connect
Resolution	Check the database. If the database is not running, start it. Once the database is up, you need to restart the Request Center Integration Server process.

Integration Server Fails to Authenticate with the Database

Error Code	LogID=1918
Error Condition	Integration Server fails to authenticate with the database.

Error Message	Exception occurred: java.sql.SQLException: [newScale][SQLServer JDBC Driver][SQLServer]Login failed for user 'RCUser'.
Resolution	Verify that the username and password parameters are configured correctly in the following configuration file: <APP_HOME>\jboss-4.2.3.GA\server\ServiceLink\deploy\requestcenter-ds.xml. If you modify this configuration file, you must restart the Service Link / ISEE application.

Sample Environment Matrix

It is a standard practice of the Universal Development Methodology (UDM) to complete a column in this matrix for each site in an implementation, as the site comes online. Cisco Advanced Services deliverables typically include a soft copy of this matrix, which administrators should keep up to date.

Table 5-1 <Client> Request Center Configuration

	Site Name/Usage (for example, Dev)
WebServer	
Front Door Portal URL	https://scdev/RequestCenter/
Admin Portal URL	https://scdevadmin/RequestCenter/
Host1:Port	
Shared Environment?	
Hardware	
Available Disk	
Operating System	
OS Login/Password	
WebServer Type/Version	
AppServer	
Host1	
Shared Environment?	
Hardware	
Available Disk	
Operating System	
Support Login/Pass	rcsupport/rc
Installer Login/Pass	requestcenter/rc
RC Path	/apps/rc
RC.ear Path	/apps/rc/RC.ear
ISEE.war Path	/apps/rc/ISEE.war

Table 5-1 <Client> Request Center Configuration

Log Path	/logs/rc
Queue Connection Factory	RCQueueConnectionFactory
BE Requisitions Queue	BEEERequisitionsQueue
BE Authorizations Queue	BEEEAuthorizationsQueue
BE Inbound Queue	BEEEInboundQueue
JDK	
JDK Path	/usr/local/java
App Container	
Type / Version	
AppHost1 RC/SL JNDI Ports	
Mail	
SMTP Server	smtpserver.domain.com
Administrator Email Address	
From Email Address	ServicePortalDev@mailserver.company.com
WebSphere WebLogic	
Console URL	
User/Password	
Node Name(s)	
Application Server	RequestCenter
Virtual host	requestcenter_host
Request Center	
Components Installed	All
Multicast IPs	225.2.2.2
Build Installed	11.2.1.0151
Admin Login/Password	
Customizations	
Patches/Hotfixes applied	
Other customizations	
Database	
Host1:Port	
Shared Environment?	
Hardware	
Available Disk	
Operating System	

Table 5-1 <Client> Request Center Configuration

OS Login/Password	
DB Type/Version	
DB SID/Database	RQSTDEV
Tablespace	RequestCenter (?GB)
Redo logs	
DB SA User/password	sa/pwd
DB RC Schema/Password	RCUser/rc
DB App User/Password	
Advanced Reporting	
Cognos Host:Port	
Cognos Hardware	
Available Disk	
Cognos OS	Windows 2008
Windows Login/Pass	rcuser/c1$c0
Admin Login/Pass	admin/admin1234
Service Account	
Paths	
Gateway Type	
Web Protocol	
Data Mart & Content Store	
JNDI Name	java:/DATAMARTDS
DB Type/Version	
DB Server:Port	
DB SID/Name	RCDMDEV
Data Mart User/Password	DMUser/dm
ContentStore SID/Name	RCCSDEV
ContentStore User/Password	CSUser/cs
Tablespace	RCDataMart (500M)
Advanced Reporting Options	
Dictionary tables	150
Service tables	50
Dictionary table pattern	DM_FDR_DICTIONARYTABLE_
Service table pattern	DM_FDR_SERVICETABLE_
Field pattern	FIELD
Dictionary Text type fields	40

Table 5-1 <Client> Request Center Configuration

Dictionary Numeric type fields	10
Dictionary Date type fields	10
Service Text type fields	80
Service Numeric type fields	20
Service Date type fields	20
Text field max size	200
Refresh WDDX for any update	Yes/No
Service Link	
Host	localhost
Queue Host:Port	localhost:5099
Base URL	http://subdomain.domain.com:80
Queue Connection Factory	RCQueueConnectionFactory
Outbound Queue	SLOutboundQueue
Inbound Queue	SLInboundQueue
JMS Queue User/Password	guest/guest
JMS File Store (WLS-only)	ServiceLinkFileStore
JMS File Store (WLS-only)	
JMS Server	RCServer

Table 5-1 <Client> Request Center Configuration

LDAP	
Server Type	
LDAP Authentication	Simple
SASL Mechanism	n/a
BindDN	
BindDN Password	
Connection Mechanism	Non-SSL
SSL Type	n/a
LDAP Host	
Connection Port	389
Secure Port	n/a
LDAP User BaseDN	
Optional LDAP filter	