Cisco Prime Service Catalog 12.0 Administration and Operation Guide

First Published: 2016-11-30

C O N T E N T S

Preface

- Preface, page xvii

Preface

Objectives

The *Cisco Prime Service Catalog Administration and Operations Guide* explains how to use the Organization Designer and Administration modules of Cisco Prime Service Catalog (Service Catalog), and how to perform basic system administration.

Organization Designer enables you to create the various departments and service teams that comprise your service request and delivery model. It is also the mechanism by which you define the roles your end-users play, and what capabilities and permissions users will receive through those roles.

The Administration module controls all site-wide settings for application behavior, including emails sent during service delivery, user interface appearance, and overall business rules for when and how to apply approvals of service requests. It also lets you define the integration with your corporate directories, and provides access to helpful utilities for troubleshooting and system maintenance.

System administrators of this application will also find this guide a valuable resource for system configuration, housekeeping, and maintenance information.

Audience

This guide is intended for system administrators, service designers, and users who are responsible for configuring the end-user administration and overall application architecture for the product.

Document Organization

The *Cisco Prime Service Catalog Administration and Operations Guide* is divided into the following six chapters:

- Structuring the Organization, on page 143: This chapter describes the Organization Designer module, the primary tool for structuring your service organization.

- Setting up User Profiles, on page 1: This chapter describes user profile personnel information, preferences, preferred language, and the work calendar.

- Configuring Site-Wide Settings, on page 201: This chapter describes the site functions in the Administration module.

- Custom Themes, on page 251: This chapter describes the capabilities provided to customize the appearance of the Service Catalog web pages.

- Maintaining Prime Service Catalog, on page 5: This chapter includes system administration, configuration management, maintenance, and troubleshooting information.

- Managing Content Deployment, on page 73: This chapter describes the content deployment and configuration management tool that is used to migrate application entities.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x	y	z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x	y	z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Convention	Indication
Choose **Menu item > Submenu item** from the X menu.	Selections from a menu path use this format. For example: Choose **Import > Formats** from the File menu.

Note   Means *reader take note* .

Tip   Means *the following information will help you solve a problem* .

Caution   Means *reader be careful* . In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver   Means *the described action saves time* . You can save time by performing the action described in the paragraph.

Danger   **Means *reader be warned* . In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

Setting up User Profiles

This chapter contains the following topics:

Setting up User Profiles

Overview

You can access personnel information, preferences, and the work calendar using User Profiles. 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.

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

Note 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.

- 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.

Language Settings

The Service Catalog 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, on page 210.

The languages that are supported out-of-box are as follows:

Table 1: Supported Languages

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

For localization of all other modules, see 'Localizing Service Catalog Strings' chapter in Cisco Prime Service Catalog Designer Guide .

Calendar

Service Catalog > Profile > 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, enter 12:00 as the starting time and 23:59 at the ending time.

- Enter 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 Catalog.

Service Catalog > Profile > Preferences can control:

- Date Formats.

- Login Module – Users can choose any module which they can access to appear automatically as soon as they log in.

- Default Service Manager View – Service performers can set the system to automatically go to the Service Manager view they use most frequently.

- 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 Service Portal 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.

Note The Service Portal module prior to version 10.0 contained the My Workspace and System module page groups by default. These pages were obsolete in 10.x and will appear if Prime Service Catalog was upgraded from 9.x versions. As an administrator, you can disable these pages by removing the read permission of the page from the **Organization Designer > Roles > Anyone** role and the pages will be hidden from all users.

- Use Service Catalog – Select the check box if you want to use the Service Catalog module.

- 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.

Viewing User's Last Login Details

You can view the user's last login details such as IP Address and Timestamp in the Prime Service Catalog user interface from the **Profile** page.

The last user login details with the specified date format is displayed on the **Profile** page.

Configuring and Viewing Security Audit Crypto Log Events

Service Catalog maintains audit log files on the Prime Service Catalog interface to track the login activities of a user.

You can configure the security audit crypto log events by enabling the option to log the security events. To do this, go to **Service Catalog > Administration > Settings** and enable the **Enable logs for Security Events** radio button. Default is off.

All the audit logs are saved in `server.log` file for all the events. The security event logs are prefixed with `SEC-AUD`.

For example:

```
COR-ID=-4724008839792176768::SEC-AUD-Fri Jan 08 12:56:31 IST 2016 : EUI Person Not found
or Imported or password error for: fdsfdsf @ 173.39.67.7:DREDDI-WS
```

To view the audit log files from the UI:

Step 1   Go to **Service Catalog > Administration > Utilities > Logs and Properties**.

Step 2   Select the **Request Center - Log Files** from the drop-down list to display all the logs available on the request center server.

Step 3   Select the **Server - Log Files** from the log to read drop-down list.

Step 4   Select the log file and click **View File** tab to view a particular log file.

Step 5   Select the number of lines from the **Last line** drop-down and click **View File**.

    Note   You can view the audit logs for a maximum of 2000 lines.

When one of the security events listed below occurs, it will be logged in the application server's log file.

- Invalid login name or password

- Forgot Password and Password Reset

- Person Profile Password Reset and Person Password Reset

- Password Warning Period

- Password Grace Period

- Password Expired and Account is Locked

CHAPTER 2

Maintaining Prime Service Catalog

This chapter contains the following topics:

Maintaining Prime Service Catalog

This chapter describes about startup and shutdown procedures for application components, recommended backup practices, configuration management and customizations of application components, ongoing maintenance tasks, and critical error conditions, error messages and resolutions

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

System Hardening

Linux Puppet Master, Linux, and Windows target VMs must have direct Internet access or through a proxy. You can alternatively configure the VM to connect with an internal repository.

The Gateway VM must be configured to route traffic as mentioned in (any specific Guide) and should not be restricted after configuration.

You must not implement firewall or SELinux rules to block specific ports after installing Puppet Master or Agents. For more information about the ports specific to applications, see (needs citation).

Note It is not recommended that you close ports in the target VM for application install. You can open ports in the Gateway VM as mentioned in Cisco Prime Collaboration Quick Start Guide.

On Linux VMs hosting Puppet Master installed with SELinux, the default installation and configuration opens the required ports (8140, 8139, and 5150) long with IPTables rules.

The Puppet Agent does not alter port access or security protocols in the VMs. Hardening these devices can cause the related applications to fail during install or run. VMs are placed in fenced containers in the UCS Director and access is controlled via a Gateway VM to prevent application failures.

Performing Backup

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

Note We recommend backing up each component as it is deployed, and saving any customizations as they are developed or modified.

- Backup operation must be scheduled regularly.

The following databases must be backed up:

- Transactional database (by default, Service Catalog)- Contains not only production data but also metadata for configuring services, service components, and other application objects.

- Analytical database- Contains data for building the standard reports, as well as the Service Catalog and Demand Center data marts.

- 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 Catalog and those written by Advanced Reporting users, as well as report views, schedules, and saved reports generated from any reports.

Tuning the Application Server

The following tuning suggestions are applicable to many Servce Catalog sites. For additional tuning suggestions, see the documentation specific to your application server.

Configuring Service Catalog 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.

To enable GZIP compression:

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

Example:

- C:\jboss-as-7.1.1.Final\ServiceCatalogServer\deployments\RequestCenter.war\WEB-INF

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

Example:

- ```
  <!--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:

Example:

- ```
  <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):

Example:

- ```
  <!--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:

Example:

- ```
  <!--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 servers.

Changing the 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. 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 Oracle 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 Catalog encounters "out of memory" errors. For example, on Weblogic the following settings have been successfully applied.

```
MEM_ARGS="-verbose:gc -Xms1024m -Xmx1024m-XX:+PrintGCTimeStamps -XX:+PrintGCDetails -XX:MaxPermSize=256m"
```

JMS Queue Connection Factory Settings

The number of connections for the queue connection factory should be configured based on the work load on the JMS server. The recommended setting for a single Service Catalog instance is 25. There is no hard and fast rule on the number of connections required based on the number of servers in the cluster. Some tuning effort may be required to arrive at the optimal connection settings for the application environment.

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).

Tuning the Database

We can list a few of the most frequently asked questions regarding how to configure and tune Service Catalog databases and the answers to those questions. For more details on these issues, you will need to see 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 Catalog 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 Catalog

- 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 the best practices of your organization.

- A very rough estimate of database storage required is 500 KB 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 Catalog 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 Prime Service Catalog 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

You can optimize performance for Oracle database in the following ways:

- Gather statistics on the OLTP database (both tables and indexes) on a regular basis. This can be automated via Oracle Enterprise Manager (OEM).

- Perform column-level histogram analysis to further optimize the Service Manager indexes.

- Gather statistics on the Service Catalog 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.

Apply settings similar to the following:

Table 2: Oracle settings

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

Enable snapshots with this command:

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

We recommend a SQLServer DBCC Reindex command, especially on volatile Service Catalog tables. The process should be regularly scheduled, typically weekly, at off hours.

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

Table 3: SQLServer commands

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.

Table 4: Cognos Database components

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

Component	# Estimated	Space per Unit (KB)	Total (KB)
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. 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.

Table 5: OLTP Database table

Prefix	Meaning	Usage
Cnf	Configuration	Tables which contain internal configuration information used by Service Catalog; 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.

Prefix	Meaning	Usage
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 that appears 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.

Optimizing Performance through Purging and Partitioning

You can optimize performance through partition and purging.

Improving Performance through Historical Requisitions Partitioning

Historical Requisition Partitioning feature moves completed requisitions, namely, requisitions that have "Closed", "Canceled", "Delivery Canceled" or "Rejected" status, to historical transaction tables. The use of Historical Requisition Partitioning provides overall application performance improvement as a result of reducing the amount of data in the current transaction tables. The improvement can be seen in the filter and search of tasks, requisitions and external messages in the Service Manager, My Services and Service Link modules. ETL and request workflow processing will also benefit from the smaller population of data in the current transaction tables.

Historical Requisition Partitioning is controlled by the system setting "**Enable Historical Requisitions Scheduler**" in the Administration module. When it is enabled, requisitions that have been completed for more than 365 days are migrated by a background process to the historical transaction tables. The 365-day retention period is configurable and may be modified based on the specific needs of your organization.

You can execute the migration process of historical requisitions on an ad-hoc basis in the **Administration > Utilities** page when the scheduler is disabled.

Thus, requisition views in both My Services and Service Manager are separated into "**Recent**" and "**Historical**" views. Requisitions migrated to the historical transaction tables can be made accessible on when you select the **Enable Historical Requisitions View** system setting. These requisitions are displayed under **Historical** tab on the **My Services > Requisitions** page, as well as **Historical Requisitions** view in Service Manager. You cannot view tasks and external messages associated with the historical requisitions through UI, although the data is stored within the Service Catalog database.

Preparing for Historical Requisition Partitioning

The first-time execution of the historical requisition migration will likely cover a large amount of data. To reduce the impact on application users, execute the process manually from the Administration module during off-peak periods:

Navigate to Administration module and ensure that the **Enable Historical Requisitions Scheduler** setting is turned off. Under **Utilities**, go to the **Run Processes**, and enter the desired cut-off date. Optionally, specify the batch size and maximum number of requisitions to process.

A larger batch size shortens the processing time but requires higher amount of temporary space or rollback segment in the database server. Setting the maximum number of requisitions or clicking **Stop** allows you to limit the duration of historical requisition migration process. The processing rate and duration vary based on the average size of the requisitions.

Note Before executing the migration process, we recommend you to work with the database administrators and perform trial runs to estimate the time required for the first-time execution.

Considerations for Datamart

Historical transaction data are not extracted by the ETL process, for Reporting. Consider the following for configuring the historical requisition partitioning feature:

- ETL process is normally scheduled to run on a frequent basis. Hence requisition data is captured into Datamart prior to their migration to the historical tables. To ensure there is no data loss in the Datamart, set the historical requisition retention period to be greater than the frequency of the ETL process. For example, if ETL is set to run every 30 days, the historical requisition retention period should be set to 31 days or more.

- The process that migrates historical transaction data is automatically put on hold when it detects that the most recent ETL process timestamp is earlier than the cutoff date. For example, if the last ETL execution was on May 1st 12pm and the migration is going to select requisitions completed before May 1st 12:30pm, the migration process will exit immediately. This ensures that data are kept in the current transaction tables for extraction into Datamart before they get migrated.

- If your organization has the need to rebuild Datamart occasionally to capture backdated data (for example, making a dictionary or service reportable after the fact), the changes will not take effect on historical transactions by re-running the ETL process. In fact, the historical data will not be recoverable in the Datamart once they have been purged. To ensure such Datamart rebuild process is still possible, configure the data retention period to a duration that has provisions for backdated changes. In addition, the Datamart should no longer be emptied in a rebuild process for the reason above. Only the portion of data that are still available in the current transaction tables can be deleted and re-inserted into the Datamart during the re-execution of ETL.

Key Settings for Historical Requisition Processing

The following settings are applicable for historical requisition partitioning:

1. newscale.properties file (located in the RequestCenter.war/WEB-INF/classes/config directory)
2. reqArchival.poller.cron - This controls the frequency of the background process that migrates historical data. It uses the standard cron syntax and is scheduled to run every 30 minutes.
3. reqArchival.process.maxRecords - This controls the maximum number of requisitions to be processed in each run. A higher number may be set if the process is intended to be run for a longer period of time during scheduled maintenance.
4. reqArchival.cutOffDate.days - This controls the retention period of completed requisitions in the current transaction tables. By default, the retention period is set to 365 days.
5. reqArchival.process.batchSize - This controls the number of historical requisitions included during each database commit. A larger batch size will shorten the processing time but will require higher amount of temp space or rollback segment in the database server.

1. support.properties file (located in the RequestCenter.war/WEB-INF/classes/config directory)

reqArchival.poller.enable - This controls whether the application instance can be used to run the historical requisition migration process. In a clustered Service Catalog environment, only one of the nodes will be used to execute the migration process at any time. One or more of the nodes may have this property set to "false" if the server is a less powerful machine or is meant for disaster recovery purpose.

Other settings in the above files should remain unchanged under normal circumstances.

Purging Requisitions

Service Catalog provides a transaction purge feature to delete transactions older than a chosen date or those that meet other user-specified criteria. This allows the application administrator to remove test requisitions before deleting test users and sample services. However, through the purge feature, you cannot perform mass data deletion. Also, you must avoid prolonged maintenance phase.

Software Requirements

- Database client for executing purge scripts

- sqlplus, for Oracle, must be installed and configured to connect to the RequestCenter database;

- osql, for SQL Server.

Preparing the System for Purging

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

Step 2   Stop the Service Catalog and Service Link services when the purge scripts are executed.

Step 3   Locate the utility in:
<APP_HOME>**schema****util****purge**

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

Step 4   Verify that the **purge** folder contains the following files:

- AddPurgeFilter.bat

- AddPurgeFilter.sh

- ClearAllPurgeFilter.bat

- ClearAllPurgeFilter.sh

- PurgeRequisitions.bat

- PurgeRequisitions.sh

Step 5   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 Catalog service packs, repeat Step 3 (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.

Purging Requisition

Purging requisition consists of the following steps:

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 canceled requisitions). However, we recommend that the criteria from the previous run are cleared initially 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

- REQUISITIONRANGE

- 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 following syntax appropriate for 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*]

Table 6: Purge filter criteria

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 PREPARATION, OPEN, ONGOING, CLOSED, CANCELLED, REJECTED, DELIVERY CANCELLED, ORDERED or ALL.
REQUISITIONID	Purge a specific requisition based on the Requisition ID.	Unique number assigned to the requisition.
REQUISITIONRANGE	Purge specific requisitions based on the Requisition ID range.	The starting and ending Requisition ID with a dash in between; for example, 30001-39999.
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.

Purge Filter Name	Description	Purge Filter Value
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.

Validating Purge Filter Criteria

Before purging requisitions, optionally perform a "dry run" to check requisitions that would be removed, without actually deleting them. This will serve as a validation for filter criteria.

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

Oracle:

PurgeRequisitions ORACLE [*SID*] [*User*] [*Password*] **DRY_RUN** [UserName]

SQL Server:

PurgeRequisitions SQLSERVER [*Server*] [*Database*] [*User*] [*Password*] **DRY_RUN** [UserName]

UserName is the Service Catalog login name of the person executing the script.

The list of requisitions found in the 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 one, 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, we recommend 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. After the purge filter criteria have been finalized, you can proceed with the actual requisition purge.

Purging Requisitions based on Filter Criteria

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 command **PurgeRequisitions** with the PURGE parameter as shown below:

Oracle:

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

SQL Server:

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

UserName is the Service Catalog login name of the person executing the script.

Purging Temporary Data

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. We recommend a practice run on sandbox environment to establish duration of the script execution 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.

Purging Workflows using the Utility on Oracle Database

To run the utility on 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 ([FromDate], [ToDate], [UserName]);

Dates must be in DD-MON-YYYY format. UserName is the Service Catalog login name of the person executing the script.

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

Example:

```
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.
```

Purging Workflows using the Utility on SQL Server Database

To run the utility on 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 [FromDate], [ToDate], [UserName]

Dates must be in DD-MON-YYYY format. UserName is the Service Catalog login name of the person executing the script.

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

Example:

```
(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
```

Purging Service Link Messages

The Service Link Message Purge Utility removes Service Link 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.

Purging Messages using the Utility on Oracle Database

To run the utility on 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 sp_CleanupSlMessageContent([FromDate], [ToDate], [UserName]);

Dates must be in DD-MON-YYYY format. UserName is the Service Catalog login name of the person executing the script.

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:

Example:

```
Updating messages with MessageStateID 2 (completed) or 3(failed) that are older than 100 daysDone
updating 3200 messagesScript Start Time 07/06/2011 02:07:11 and script End Time07/06/2011 02:09:11
```

Purging Messages using the Utility on SQL Server Database

To run the utility on 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_PurgeWorkflowTables [FromDate], [ToDate], [UserName]

Dates must be in DD-MON-YYYY format. UserName is the Service Catalog login name of the person executing the script.

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

Example:

```
Purge messages with MessageStateID  2 (completed) or 3 (failed)
Done updating 1500 messages
Script Start Time Jul 6 2011 2.57 PM and script End Time  Jul 6 2011 3.57 PM
```

Managing Undelivered Emails

Email notifications that failed to be delivered are kept in the application for review or retry. To delete or resend, navigate to the Administration module, and locate the "Undelivered Emails" tab under Utilities. Delete the messages if they have invalid information, or re-send them if they failed to be delivered due to temporary SMTP outage.

As a good practice, administrator should review this application page on a regular basis to identify messages that need to be re-sent. Email notification process may slow down substantially if there is a large number of messages left in the backlog.

Modifying the First Day of the Week for the Weekly Usage Reports

By default, the weekly usage reports displays the first day of the week as **Monday**. To modify the first day of the week for the weekly usage reports, do the following :

Step 1   Log into your database server as an administrator and run the following query :
Delete from RpWeeklyUsageDetails

Step 2   Edit the **reportsdata.import.beginnerofweek** attribute in the **newscale.properties** file, for example,

Example:

- `reportsdata.import.beginnerofweek= Sunday`

The **newscale.properties** file is located in the **RequestCenter.war/WEB-INF/classes/config** directory.

Managing Different Application Servers

This section provides information about maintaining the application, and managing WebLogic, and JBoss. 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.

For a typical installation using the JBoss application server, Cisco Prime Service Catalog is started and stopped along with the application server on the command line or Windows services, if they are configured.

Detailed information about starting WebLogic can be found in the Cisco Prime Service Catalog Installation and Upgrade Guide.

The admin server should not need to be restarted during regular Service Catalog 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.

To restart your system:

Step 1   Choose **Start** > **All Programs** > **IBM Cognos 8-64** > **IBM Cognos Configuration**.

Step 2   Choose **Actions** > **Restart**.

Restarting using Windows Services

Stop the following service and then restart:

- IBM Cognos 10.2.1 – required for all reporting options

Deploying the Application

The .war file for Service Catalog is deployed into the file system. The exact location of these files will vary, depending on application server. The Service Link application is provided as a .war file, ISEE.war (Integration Server Enterprise Edition.).

Startup and Shutdown Procedures

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

- Cisco Prime Service Catalog application

- Cisco Prime Service Catalog Integration Server (Service Link)

- Reporting Server

Restarting Prime Service Catalog, Service Link, and Reporting Servers

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

Key Configuration Files

The following are important files that you may need to see 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.

File	Description
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.war\WEB-INF\classes\config" folder. As such, the file is redeployed any time the .ear file is redeployed. The Service Catalog administrator should preserve the data contained in the file, but should not 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 • ObjectCache.Application.URL – URL reference back to the application 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

File	Description
rcjms.properties	This file is also located in the "RequestCenter.war\WEB-INF\classes\config" folder. It contains the JMS settings for application internal communications. Please ensure that the queue names match the ones on the application server.
integrationserver.properties	This file is located in the "ISEE.war\WEB-INF\classes\config" folder. It contains the key properties of the integration server (Service Link).

Managing Logs

Service Catalog 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.

We recommend that you:

- Rotate logs on a daily basis (this is the default behavior)

- Keep one month of logs "online"

- Back up or delete logs that are older than a company-specified retention period

Service Catalog does not require log files to be maintained. They are useful primarily as troubleshooting tools in case an error arises. There are four types of log entries: **E** (Error), **W** (Warning), **I** (Info), **D** (Debug), listed in decreasing order of severity.

We recommend against changing the format of the default log files because that is 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 are written to the ServiceLink\logs directory:

- dbadapter.log

- fileadapter.log

- httpadapter.log

- msadapter.log

- mqadapter.log

- remedyadapter.log

- vmwareadapter.log

- wslisteneradapter.log

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. For more information, see Logs and Properties, on page 236.

WebLogic Logging

In WebLogic, Cisco Prime Service Catalog 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 "<JBOSS_DIR>/standalone/log" folder. The logging.properties file that determines logging behavior is located under the "<JBOSS_DIR>\standalone\configuration" folder. Log4j.xml is no longer used for controlling application logging.

Configuring 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.

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 Catalog (for example, a SQLServer data source accessed from an instance of Service Catalog running on Oracle, or a Sybase data source accessed from any instance of Service Catalog) is not supported in a service form. Procedures for configuring data sources are detailed in the Cisco Prime Service Catalog Installation Guide, and are specific to the application server.

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

You can configure a custom data source using JBOSS 7.1.1.

Step 1 Log on to the JMX admin console of JBOSS Application Server.

Step 2 Choose **Datasources**.

Step 3 Select **Validation** tab.

Step 4 Enter the following data in the **Valid Connection Checker** field.

- Select 1 (for SQL server)
- Select 1 from dual; (for Oracle server)

Note		You must populate and enable Valid Connection Checker while configuring Datasources to prevent intermittent SQL disconnections.

Step 5	Uncheck the **Validate on Match** check box to make it false.
Step 6	Check the **Background Validation** check box to make it true.
Step 7	Enter **Validation Millis** as 600000.
Step 8	Click **Save**.
Step 9	Select **Pool** tab.
Step 10	Enter the **Min Pool Size** as 1 and **Max Pool Size** as 10.
Step 11	Click **Save**.
Step 12	Select **Properties** tab.
Step 13	Enter the **Strict Minimum** and **Prefill Enabled** values as True.
Step 14	Click **Save**.

Creating Backing Tables for External Dictionaries

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

For the application 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;
```

Configuring Service Export via SSL or NTLM

The Service Export feature in Service Designer establishes a connection to Service Catalog, 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 the application needs to authenticate to the server, and the Service Catalog needs an SSL certificate.

To enable the export service feature when Service Catalog is SSL-enabled:

Step 1   Export the trusted root CA certificate used by the Service Catalog web server, in Base 64 Encoding format, into a file. The file will 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 application server. The CA certs keystore for your Java installation is a file named cacerts.

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

Step 3   Import the trusted root CA certificate of the Service Catalog web server into the Java's cacerts keystore. You can also use the Java keytool utility.

- The keytool.exe program can be found in the <JAVA_HOME>/bin directory.

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

Example:

```
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 Service Catalog 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**.

Step 4   Restart the application server instance, for the changes to take effect. Restart the whole instance of JBoss WebLogic in this machine, and not just an individual server or application.

Reloading Cached Data 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 **Update**. This invalidates the cache and reloads the settings from that page.

Business Engine Caching

Cisco Prime Service Catalog 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 occur 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, where you can:

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

Other caching mechanisms are also in place within the application. The cached values are refreshed automatically as and when changes are made to the application data.

Securing Prime Service Catalog Database

User passwords are usually not stored in the database if external authentication via SSO is used. When they are, they are a one-way AES 128-bit 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.

Local application 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 are not encoded; data-level security verifies authorization for each screen.

Securing Application

This section describes about the application security:

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

Service Catalog maintains a password-protected key-store that can store many certificates.

We recommend 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.

Removing 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.

Service Catalog 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\.

Form Data Security

For installations that are on release 9.3.2 and later, there are a number of service design features that can be used to protect service requests from the malicious files. To prevent malicious attempts to intercept form data that are governed by form rules and default value settings, server-side rules and certain edit controls can be used to override or validate data being sent from the browser clients. For more information, see Cisco Prime Service Catalog Designer Guide.

Reporting Batch Programs

The Reporting modules require scripts that maintain the Service Catalog data mart and produce the standard reports and KPIs available to users.

Service Catalog Extract-Transform-Load (ETL) scripts generated from the Cognos DataManager ETL tool controls the population of the database which supports running prebuilt reports provided by Service Catalog and all nonform 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 Service Catalog data mart.

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 <ReportingInstalledDirectory>\logs directory of the Cognos server.

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

Table 7: Support standard report

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

The following programs are required to support the data marts.

Table 8: Support data mart

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 creates 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 Catalog 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 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
```

Monitoring Tasks using Escalation Manager

The Escalation Manager is responsible for monitoring if 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 newscale.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".

Fulfilling Service Requests using Service Manager

Service Manager is the module used by task performers 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 is not recommended as it will impact Service Manager 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
```

For the changes to take effect for the newscale.properties files, navigate to the **Administration > Utilities** modules, select "Request Center – Property Files" from the drop down, select "newscale.properties" file and click the "View File" button. Review the file content to make sure it includes your changes, and then click the "Reload" button. Click "OK" button when the reload success message is displayed.

Installation Log Files

Installation Logs are saved to the <APP_HOME>/logs folder with a mmddyyyyhhmm time-stamp (for example, 010720111126) each time the Installer is invoked.

Key installation logs are listed below.

Table 9: Installation log files

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.

File Name	Contents
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.

Installation settings are recorded in the RequestCenter/etc folder. Preserve that folder so that installation settings are stored for future invocations of the Service Catalog Installer.

The settings are available in the file setup_options.txt.

Multicast Settings

A single clustered installation of Cisco Prime Service Catalog 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.

Service Catalog uses multiple multicast addresses that have to be unique.

Testing Multicast Connectivity

This section describes how to test multicast connection. You can perform a test to check if Node1 can talk to Node2, as follows:

1 Choose a valid multicast address and port that are not in use.
2 On Node2: java -classpath .:./javagroups-all.jar org.javagroups.tests.McastReceiverTest -mcast_addr 224.10.10.10 -port 5555.
3 On Node1: java -classpath .:./javagroups-all.jar org.javagroups.tests.McastSenderTest -mcast_addr 224.10.10.10 -port 5555.
4 On Node1 you see a prompt ">".
5 Type in some text and press Enter.
6 Your text appears on Node2.

You can also check if Node2 can talk to Node1:

Repeat the procedure (test) stated above with Node2 as the Sender and Node1 as Receiver.

For managing integration, the key integration strategies that the system administrator must pursue when configuring the Service Catalog application are described in Cisco Prime Service Catalog Integration Guide .

Directory Integration

The system allows for multiple LDAP directory integrations. A group of two or more LDAP sources becomes one LDAP system through referrals. Referrals are supported for searches only, not binding. For detailed information on configuring directory integrations, see the Cisco Prime Service Catalog Integration Guide .

Directory Integration allows integration architects to connect Service Catalog 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 Catalog. Events that can trigger an LDAP lookup include:

- Authentication after login, either via the Service Catalog 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 managers of a person previously chosen via Order on Behalf or Person Search

In addition to these preconfigured 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 Catalog uses the server default. Also, if any optional fields are not mapped, any value previously populated in the Person profile remains unchanged.

Custom Mappings

Custom mappings can be created via pattern-matching language (regular expressions), which is described in the Cisco Prime Service Catalog 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 Catalog instance is migrated or upgraded.

Custom Code

Using the interfaces provided by the Directory Integration API, custom Java classes can replace or supplement the preconfigured 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.

Troubleshooting Single Sign-On

Single Sign-On functionality is provided as part of Directory Integration. 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.
- Check if the Service Catalog is still accessible through the Administrative override
- Restart the Service Catalog 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 Catalog
- Configure SSO to strip DOMAIN information

Interactive Service Forms (ISF)

ISF is a JavaScript API that integrates with Cisco Prime Service Catalog service forms. ISF allows the forms to dynamically alter their contents or behavior based on the current context, including user credentials; data previously entered on the form; or the life cycle of the displayed requisition. For more information on ISF, see the Cisco Prime Service Catalog Designer Guide .

ISF supports the use of JavaScript libraries, stored on the application or web server, to supplement JavaScript code stored in the Service Catalog repository. If such libraries are used, they are treated as customizations when upgrading or migrating a Service Catalog site.

Retrieving Data using Active Form Components

The data retrieval rules available within active form components allow the application to retrieve data from external relational databases or from the application database, for use in service forms. Such data can be used to prefill 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 Prime Service Catalog Installation and Upgrade Guide. Any such datasources are treated as customizations when upgrading or migrating the Service Catalog site.

Integrating with External Systems using Service Link

Service Link, also known as the Integration Server, or ISEE (Integration Server Enterprise Edition), allows Service Catalog 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

This section provides information about configuring your system for a customized installation of Service Catalog, and ensuring that custom content is not deleted or overridden during subsequent installations or upgrades.

For more details on the Service Catalog installation wizard, see the Cisco Prime Service Catalog Installation and Upgrade Guide .

How the Installer Works

The Service Catalog installation wizard builds the WARs and:

- Expands the core product WAR

- Modifies .properties files based on settings chosen during installation

- Merges in a customizations file, if one is specified as part of the installation parameters

- Rejars the WAR

- Publishes the WAR to the dist/folder for deployment

The deployment procedure stipulates that an entire WAR file be deployed to a server. When an entire WAR file is deployed, the previous directory where the WAR was expanded is wiped clean, and any Service Catalog customizations that existed in the directory are lost.

To avoid losing the customizations, the Service Catalog installation wizard allows you to specify custom content to be included in the installation:

Procedure

Step 1 Create an archive containing the custom content in the Zip format. The archive directory structure must match the deployment directory structure.

Step 2 Run the Service Catalog installation wizard as described in the Cisco Prime Service Catalog Installation and Upgrade Guide, using the **Advanced Installation** type.

Step 3 On the Application Server Configuration page, click **Advanced Options**.

Step 4 In the The Advanced Options dialog box, select **Custom content**.

Step 5 Enter the full path in the **Custom content archive** including the name of the archive, or click **Browse** to locate and choose the custom content archive.

Step 6 Click **Close**. Continue with the installation as described in the Cisco Prime Service Catalog Installation and Upgrade Guide .

While the Service Catalog installation wizard completes the installation, it extracts your custom content archive into the application deployment directory structure.

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:

Table 10: Custom components

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
	rcjms.properties
	integrationserver.properties
	newscalelog.properties

Database Scripts

We do not recommend modifying the database outside of the APIs provided by Cisco. However, some scripts may need execution 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 reinstall.

Managing Configuration using Catalog Deployer

A Service Catalog implementation typically consists of multiple sites, each of which plays a different role:

Table 11: Multiple sites

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 Catalog Deployer module provides configuration management for metadata (service definitions) and organizational data (people, organizations, and related entities) which is stored in the repository. For more information, see Cisco Prime Service Catalog Designer Guide for Catalog Deployer documentation.

Copying a Database

You can copy Service Catalog OLTP database from one site to another during deployment, for instance:

- 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.

Perform the following procedures to copy a Service Catalog OLTP database from one site to another.

Exporting Source Database

Step 1   Inform the users of expected downtime.

Step 2   Stop the Service Catalog 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 Service Catalog and Service Link services.

Importing Database to Target Site

Step 1   Stop the Service Catalog 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.

      Note   For SQLServer, ensure that logins and users exist in the newly imported database match the credentials required for this instance of Service Catalog. If required, create a new login 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 Catalog installer.

Step 5   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 6   Restart the Service Catalog and Service Link services in the target environment.

Step 7   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 8   If the two sites are connecting to two different LDAP directories, adjust the Directory Integration Data Source definition appropriately.

Step 9   Check and modify any connection properties for the Service Link agents as appropriate for the target environment.

Step 10   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 11   Inform users that the maintenance is complete.

Configuring SSL for Service Link Inbound Documents

This section describes about configuring SSL for service links.

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 section.

Note Service Link, as a server, does not support client certificate authentication during SSL handshake.

Enabling SSL for Service Link

Enabling SSL for Service Link turns on the secure port, but it does not turn off the nonsecure port for Service Link. If you choose not to turn off the nonsecure port, external systems can still communicate with Service Link via an http URL. If you decide to turn off the nonsecure port, all communications with the Service Link service must use the **https** URL.

It is possible to use both secure and nonsecure port for the Service Link service and control the access to the nonsecure port via another mechanism, such as a firewall system.

For example, in a Two-JBoss-Server topology, the Service Catalog application is also a "client" of the Service Link service (which runs on a separate JBoss server). At runtime, Service Catalog needs to connect to the Service Link service via the URL http://<*SL_servername*>:6080. If the nonsecure port 6080 is turned off for the Service Link service, then Service Catalog must be configured to connect to Service Link via an https address, that is, **https**://<*SL_servername*>:**6443**.

So, one possible scenario is that you turn on both nonsecure port 6080 and secure port 6443 for the Service Link service. Service Catalog can still connect to Service Link via http://<*SL_servername*>:6080, while other external systems must only communicate with Service Link via https://<*SL_servername*>:6443. You configure your firewall system to deny access to port 6080 from all external systems.

This section does *NOT* describe how to turn off a nonsecure port for the application server or how to configure a firewall system to deny access to a nonsecure port number. Please contact your system administrator, or the vendor of your application server product to obtain the information you need.

If Service Link is deployed in a separate application server from Service Catalog (as in the case of a clustered WebLogic environment, or in the case of a Two-JBoss-Server topology), then to enable SSL for Service Link, you configure the certificate and secure port number only for the application server where Service Link is running.

Creating a Certificate Keystore

It is assumed that you have procured 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.

> **Note** This document does not describe how to create a keystore file, and how to request a certificate for your web server or application server. The instructions in this section assume that you have already created a keystore file that contains the digital certificate to be used to enable SSL for the application server where Service Link is running. For ease of documentation, 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**".

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 is similar to the following example:

```
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCBE17w1cwDQYJKoZIhvcNAQEEBQAwZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNB
MRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG5ld1NjYWxlMQswCQYDVQQLEwJRQTEVMBMG
A1UEAxMMS2hhbmcgTmd1eWVuMB4XDTExMDMxMjE5MDI0N1oXDTIxMDMwOTE5MDI0N1owZTELMAkG
A1UEBhMCVVMxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG5ld1Nj
YWxlMQswCQYDVQQLEwJRQTEVMBMGA1UEAxMMS2hhbmcgTmd1eWVuMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDhTxg2RwarD6Wn4iqYeOOk3ykfXzZiDArf/X63omXquTmN0Up+mg6oJmPAfqJA
l7k4+Dn7dfVtAc4h8qra7PBeBU48zrzRqZd6VAK07rz++CilQto64mHXYVomb5vWPGeKA41j9vlv
ENj/tE/6++IqbwnxAqeZtY3EvEM7dcCWDwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAAaqCnfEAovy
Uf2S+oAXYDo5N387a035APsz5iiUM5oiKR/KW3oRz/v0P0I/o3n312kDIJ01111pl6qpZRtPEsr1
b00Tu1cXfPmizEtz0ole606qDS+DzkS1+YYz2mLL2Zq40d1EPsMolyqyUmyq3GHaEnuhWemcv2aA
wGFgbQYd
-----END CERTIFICATE-----
```

Skipping Certificate Validation

You could choose to skip the certificate validation for an SSL connection by checking the **Skip Certificate Validation** option when you create a connection. When this option is selected the Certificate validation is skipped and the connection is established without the Certificate Keystore information.

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.

For JBoss 7.1.1

Step 1 Stop the JBoss server where the Service Link application is running.

Step 2 Copy the "**slkeystore.jks**" file into the "<JBOSS_DIR>\ServiceLinkServer\configuration" directory, where <JBOSS_DIR> is the installation directory of the JBoss server where the Service Link application is deployed.

Step 3 Make a back up of file "<JBOSS_DIR>\ServiceLinkServer\configuration\standalone-full.xml". Use a text editor to open file "standalone-full.xml". Ensure you use a text editor that will not insert any special carriage return characters or any other formatting characters into the file.

Step 4 Search for the following line in file "standalone-full.xml":

Example:

```
<connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
```
Insert the following three lines right below it:

Example:

```
<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
<ssl name="ssl" key-alias="servicelink" password="slpassword"
certificate-key-file="../ServiceLinkServer/configuration/slkeystore.jks"/>
</connector>
```

Note In the above entries, it is assumed that the name of your keystore file is "slkeystore.jks", the alias for the certificate is "servicelink", and the password to open the keystore file is "slpassword".
Search for the following string in file "standalone-full.xml":

Example:

```
<socket-binding name="https" port=
```

Step 5 Make a note of the value for port number. This will be the secure port number used by the JBoss server in SSL mode.

Step 6 Stop the JBoss server where the Service Catalog application is running, and Navigate to the "<JBOSS_DIR>\ServiceCatalogServer\deployments\RequestCenter.war\WEB-INF\classes\config" directory.

Step 7 Use a text editor to open file "newscale.properties", and search for the following parameter:

Example:

```
isee.base.url=
```
Note The Service Catalog application is communicating with the Service Link application via this URL. This Service Link URL is now SSL enabled, and thus the address needs to be changed to an https address, and the port number needs to be changed to the secure port number used by the JBoss server for Service Link.

Step 8 Change the value for this parameter from http://<hostname>:<nonsecure_port_number> to **https**://<hostname>:**secure_port_number**.

Step 9 Copy file "slsigner.cer" to the "<JAVA_HOME>\jre\lib\security" directory, where <JAVA_HOME> is the JDK 6 installation directory.
It is assumed that file "slsigner.cer" contains the CA certificate.

Step 10 Open a Command Prompt window or a Console window and navigate to the "<JAVA_HOME>\jre\lib\security" directory.

Step 11 Execute the following command to import the CA root certification into the trusted certificate keystore used by JDK 6:

Example:

```
<JAVA_HOME>\bin\keytool -import -trustcacerts -file slsigner.cer -alias servicelink -keystore cacerts
 -storepass changeit
```

Note In the above entries, it is assumed that "slsigner.cer" is the name of the file that contains the CA root certificate, "servicelink" is the alias, "cacerts" is the name of the trusted keystore file for JDK 6, and "changeit" is the password to open the "cacerts" keystore file.

Step 12 Start both ServiceCatalogServer and ServiceLinkServers, and connect to the Service Catalog URL as an administrator user, or as a user who can access the Service Link module.

Step 13 Open the Service Link home page, in the Service Link Status section, verify that the connection is in green status, and both the SSL icon and the secure port number are displayed.

Step 14 Any external system that sends an inbound document to the Service Link agent that uses the HTTP/WS adapter will need to be updated as follows:

a) The inbound routing URL needs to use the https address and the secure port number.

b) The signer certificate for Service Link (contained in file slsigner.cer) will need to be imported into the trusted CA root certificate keystore of the external system.

For WebLogic 10.3.6

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:\Program Files\Java\jdk1.7.0\

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, and click the **Configuration >Keystores** subtab.

Step 4 On the Keystores page, enter the following values.

Note Replace *<JAVA_HOME >* with the full pathname of the Java Directory. (For the read-only fields, verify the values that appear are correct.)

Table 12: Keystore fields

Field	Value
Keystores	Custom Identity and Java Standard Trust
Custom Identity Keystore	*<JAVA_HOME >*\lib\security\slkeystore
Custom Identity Keystore Type	jks

Field	Value
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 5   Click **Save**, and click the **Configuration > SSL** subtab.

Step 6   On the SSL page, enter the following values:

Table 13: SSL fields

Field	Value
Identity and Trust Locations	Keystores
Private Key Alias	servicelink
Private Key Passphrase	slpassword
Confirm Private Key Passphrase	slpassword

Step 7   Click **Save**, and click the **Configuration > General** subtab.

Step 8   On the General page, enter the following values:

> • Check the **SSL Listen Port Enabled** check box.

> • SSL Listen Port = *<enter an available port number, for example 9443 >*.

Step 9   Click **Save**, restart the WebLogic server where Service Link is deployed.

Step 10   Check if the log file "*<WL_servername >*.out" contains messages similar to the following, to ensure that the WebLogic server has started in the secure port (9443):

Example:

```
<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 11 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:

Example:

```
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:

Example:

```
<JAVA_HOME>\bin\keytool –printcert –file slsigner.cer
```

Step 12 If you decide to disable the nonsecure 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 must be changed from http to **https** address with the secure port number. For example, previously, the Service Link URL may be:

Example:

```
http://<sl_servername>:9001/IntegrationServer/ishttplistener/ <agent_name>
```
It must be changed to:

Example:

```
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

Step 1 environment To disable the nonsecure port for the Service Link service, you must import the signer certificate into the *Java Trusted Certificate Authority Keystore* of the Service Catalog service.
This is because Service Link runs a separate WebLogic server that does not belong to the cluster. (Only Service Catalog and the Business Engine can be installed on the cluster.) Service Catalog acts as a "client" that connects to the Service Link service at runtime.

Step 2 Complete the following procedure to import the signer certificate into the *Java Trusted CA Keystore* for Service Catalog:

a) Log on to one of the nodes of the WebLogic cluster where Service Catalog 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:

Example:

```
set JAVA_HOME=C:\jdk170
```

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:

Example:

```
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 Service Catalog 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:

Example:

```
isee.base.url=http://<hostname>:9001
```
and change it to:

Example:

```
isee.base.url=https
://<hostname>:9443
```

g) Repeat Step (f) for every node in the WebLogic cluster where Service Catalog is deployed.

h) Restart the WebLogic cluster for Service Catalog.

To avoid Step 1 entirely, you may decide to turn on both the nonsecure and secure ports for the Service Link service. This way the Service Catalog application can still connect to Service Link using the nonsecure URL (http://*<hostname >*:9001), however, ou may want to consider taking some measures (such as a firewall system) to block access to the nonsecure port from all external systems.

Configuring SSL for Service Link Outbound Documents

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 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 detail.

- Specifying the Outbound URL for SSL, on page 48

- Importing the Signer Certificate to a Trusted CA Keystore, on page 49

- Configuring JBoss 7.1.1, on page 49

- Configuring WebLogic 10.3.6 (11g), on page 50

Specifying the Outbound URL for SSL

Step 1   Log on to Cisco Prime Service Catalog as a user who can access Service Link, navigate to the Service Link module and click the **Manage Integrations** tab.

Step 2   Choose the agent that you want to configure, open the Outbound Properties page of the agent.

Step 3   In the **HttpOutboundAdapter.RoutingURL** field, enter the https address with the secured port number, for example, https://192.168.21.202:8444/HTTPSimulator/.

Step 4   Set the value for the **HttpOutboundAdapter.AcceptUntrustedURL** field to **false** to ensure a secure connection.

Step 5   Click **Save**, open the Control Agents tab, and restart the agent.

Importing the Signer Certificate to a Trusted CA Keystore

Before following the application server-specific instructions, you must complete the following step:

Note If the signer of the external web server certificate is a well-known Certificate Authority like VeriSign or Thawte, then most likely, you can skip this step since Sun JDK already recognizes CA signers.

- Obtain 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
MRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG5ld1NjYWxlMQswCQYDVQQLEwJRQTEVMBMG
A1UEAxMMS2hhbmcgTmd1eWVuMB4XDTExMDMxMjE5MDI0N1oXDTIxMDMwOTE5MDI0N1owZTELMAkG
A1UEBhMCVVMxCzAJBgNVBAgTAkNBMRIwEAYDVQQHEwlTYW4gTWF0ZW8xETAPBgNVBAoTCG5ld1Nj
YWxlMQswCQYDVQQLEwJRQTEVMBMGA1UEAxMMS2hhbmcgTmd1eWVuMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDhTxg2RwarD6Wn4iqYeOOk3ykfXzZiDArf/X63omXquTmN0Up+mg6oJmPAfqJA
l7k4+Dn7dfVtAc4h8qra7PBeBU48zrzRqZd6VAK07rz++CilQto64mHXYVomb5vWPGeKA41j9vlv
ENj/tE/6++IqbwnxAqeZtY3EvEM7dcCWDwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAAaqCnfEAovy
Uf2S+oAXYDo5N387a035APsz5iiUM5oiKR/KW3oRz/v0P0I/o3n312kDIJ01111pl6qpZRtPEsr1
b00Tu1cXfPmizEtz0ole606qDS+DzkS1+YYz2mLL2Zq40d1EPsMolyqyUmyq3GHaEnuhWemcv2aA
wGFgbQYd
-----END CERTIFICATE-----
```

The instructions for importing the signer certificate depend on the application server (Configuring JBoss 7.1.1, on page 49, Configuring WebLogic 10.3.6 (11g), on page 50, or Troubleshooting, on page 50) that Service Link is running on.

Configuring JBoss 7.1.1

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.

Step 3 Import the signer certificate into the "cacerts" keystore by executing the following commands in a Command Prompt window or a Console window:

Example:

```
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 "keytool" 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.

Configuring WebLogic 10.3.6 (11g)

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:

Example:

```
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 "keytool" 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.

Troubleshooting

This section provides information about how to limit outbound email and to control email generation. It also includes information about contacting Cisco with support questions and methods for keeping track of your system environment and error information.

Tracking and Troubleshooting Application Provisioning Process

After you order the application template, the orchestration component provides an option to track the template provisioning progress in **Comments and History**, under My Stuff.

If the (built-in) Cloud orchestration service is restarted when Prime Service Catalog is running, it reconnects to Prime Service Catalog, discovers AMQP exchanges, and resumes monitoring of AMQP messages.

Whereas, if Prime Service Catalog is restarted when Cloud orchestration service is running, the Cloud orchestration service reconnects to Prime Service Catalog when it resumes execution.

When an order (for the application template) is submitted, the Cloud orchestration engine (Heat Engine) status is checked before the engine starts provisioning the application template:

If the Cloud orchestration engine or the Cloud orchestration engine API service is down, the Cloud orchestration service cancels the requisition in Prime Service Catalog and logs in **Comments** for that requisition: `Heat Engine service is down. Details: <More information on the service status>.`

Note   Cloud orchestration engine is not fault tolerant: If it goes down when an infrastructure template is being provisioned, the provisioning is halted and cannot be recovered when the engine is restarted at a later point.

Restarting Cloud Orchestration Engine and Orchestration services

Enable root access from the Shelladmin Menu, login as root (using the Shelladmin menu option), run the following commands, view log files and so on. (Alternatively, using the Display Service Status option, you can view the status for all services including the following services):

```
sudo service openstack-keystone restart
sudo service openstack-heat-api restart
sudo service openstack-heat-api-cfn restart
sudo service openstack-heat-engine restart
sudo service amqp-service restart
sudo service psc-orchestration restart
```

Log Files

You can examine orchestration service and heat engine logs under **Administration > Utilities > Logs and Properties**, and choose **Request Center - Log Files**.

  • Orchestration logs are located in /var/log/cisco/psc/psc-orchestration.log

  • Cloud Orchestration (Heat) engine logs are located in /var/log/heat/engine.log

Commonly Monitored Traces

The following traces are commonly monitored:

Database Interactions	com.newscale.bfw.udkernel.udsql.UdSqlBean
	com.newscale.bfw.udkernel.util.UdKernelUtil
LDAP Interactions	com.newscale.bfw.ldap.jldap.JLDAPApi
Clustering Issues	net.sf.ehcache.distribution.jgroups.JGroupsCacheManagerPeerProvider

Limiting Outbound Email

You may want to limit outbound email during service design testing or in nonproduction 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.

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 nonproduction 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 do not have to change Service Catalog 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 users 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

Service Catalog 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 as it has a minimal negative effect on CPU and network bandwidth usage. This is enabled via a setting in the newscale.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 10 times (by default) and are configured by the Email.ServerDownCount property. The connection retries to the SMTP host are paused for the configured time (in msec) specified in the Email.RescheduleOffset property.

In addition, issues such as configured mailbox exceeding the set limit, email bounces, or other delivery problems are retried based on the default setting of the Email.RetryCount property (currently, the default is 4).

Environment/Platform Overview

It is useful to document the systems in your environment by using a matrix like the one provided in the .

Cisco publishes a support matrix detailing the software on which each version of Service Catalog 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.

Contacting Cisco Technical Assistance Center (TAC)

You can 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 Catalog 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

This section describes about gathering troubleshooting information in various situations.

Site Debugging

If an "Our Apologies" exception occurs, you may turn on "Debug" via the Debugging option of Administration module Settings.

Figure 1: Debugging page

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.

Figure 2: URL at the bottom
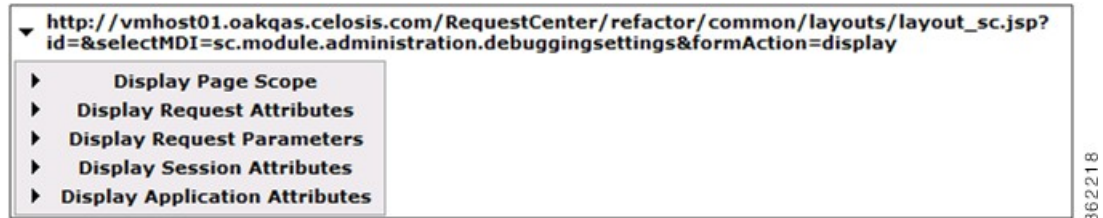
When you are finished, turn off the debugging, as it may confuse end-users. It also adversely affects performance.

The application log is a key troubleshooting mechanism. Checking 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 Service Catalog 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 cases, 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.

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

Enabling Adapter Log Files for ServiceLink Application

On WebLogic, the log files for the ServiceLink adapters are not enabled by default. By default, all logging for ServiceLink adapters are written to the server.log file for the WebLogic server.

This section describes the configuration steps to enable the adapter log files for ServiceLink. These configuration steps must be performed manually by the user after the ServiceLink WAR is deployed.

Note This section is not applicable for JBoss, since the Service Catalog Installer automatically configures the ServiceLink adapter log files at installation time.

For WebLogic 11g

Step 1 If the ServiceLink application is deployed and running on the WebLogic server, stop the WebLogic server. You cannot stop just the ServiceLink application; you must stop the entire WebLogic server.

If you have not deployed the ServiceLink application, then follow the steps up to the point where you have to extract "ISEE.war" into a ServiceLink directory. (Remember that you must deploy ServiceLink in an extracted WAR format.) Next, perform the steps described in this section in the extracted ServiceLink directory, before you begin the deployment. In other words, in Step 3 below, you navigate to the extracted ServiceLink directory, instead of the staging directory.

Step 2 Log in to the machine where ServiceLink WAR is deployed.

Step 3 Navigate to the directory "<BEA_HOME>\user_projects\domains\<domain_name>\servers\<server_name>\stage\ServiceLink\WEB-INF\classes\config".

Step 4 Use a text editor to modify file "newscalelog.properties" as follows:

1 Make sure that the line "logger.class.name=com.newscale.bfw.logging.LogUtilCommonsImpl" is not commented out.

2 Remove the comment sign in front of "logger.directory=", then enter the correct log directory for the WebLogic server where ServiceLink application is deployed. This should be the directory where the "server.log" for the WebLogic server is located. For example,

On UNIX or Linux:

logger.directory=/opt/bea/user_projects/domains/mydomain/servers/server1/logs

On Windows:

logger.directory=C:/bea/user_projects/domains/mydomain/servers/server1/logs

Note On Windows, use the slash (/), instead of the backslash (\) as the directory delimiting character.

Step 5 Start the WebLogic server.

In the same directory for "server1.log", you can see a new log file called "isee.log", and several additional log files – one for each ServiceLink adapter.

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

See also,

Error Log Locations

Error logs for Service Catalog and its related components are in the following locations:

Table 14: Error log path

Component	Error Log Location
Application Server	
WebLogic	<BEA_HOME>/user_projects/domains/<domain>/servers/ <server>/logs/<server>.log
JBoss	<JBOSS_HOME>/ServiceCatalogServer/log, <JBOSS_HOME>/ServiceLinkServer/log

If you have configured the support utilities in Administration module to enable GUI access to the application log files, you can also view and download the above log files from there.

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 Service Catalog server log file, whose behavior and location are described earlier.

Failure to perform Asynchronous Submit/Authorization

Table 15: Submit/Authorization errors

Category	Description
Error Condition	Service Catalog is not able to instantiate a task plan asynchronously, after the request submission 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 Service Catalog queue that processes these tasks is temporarily unavailable. Please try again later or contact your Service Catalog 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

Table 16: Connection loss errors

Category	Description
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.

Failure to Connect to the LDAP Server – Incorrect Port

Table 17:

Category	Description
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 Service Catalog application.

Failure to Connect to the LDAP Server – Incorrect Hostname

Table 18:

Category	Description
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>

Category	Description
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

Table 19:

Category	Description
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

Table 20:

Category	Description
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

Category	Description
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

Table 21:

Category	Description
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 Service Catalog application server.

Failure to Connect to the LDAP Server

Table 22:

Category	Description
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 Service Catalog application server.

Failure to Authenticate with the LDAP Server

Table 23:

Category	Description
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 Service Catalog application server.

Attribute Name is Mapped Incorrectly

Table 24:

Category	Description
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 Service Catalog application server.

User Base DN in LDAP Server is Missing

Table 25:

Category	Description
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

Table 26:

Category	Description
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 "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

Table 27:

Category	Description
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.

Category	Description
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

Table 28:

Category	Description
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. Choose a correct value for the "Common OU for new users" field.

User Cannot be Found in the LDAP Server

Table 29:

Category	Description
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

Table 30:

Category	Description
Error Condition	Cannot connect to one of the Referral LDAP Systems. (The config flag SkipErrorOnLDAPSystem=true; thus, Service Catalog 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

Table 31:

Category	Description
Error Condition	Cannot connect to the External Data Dictionary Database.

Category	Description
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 Service Catalog application.

Lost Connection to the Database

Table 32:

Category	Description
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.

Failure to Connect to the External Data Dictionary Database

Table 33:

Category	Description
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.

Category	Description
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 Service Catalog 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 34: Client Service Catalog Configuration

Category	Site Name/Usage (for example, Dev)
WebServer	
Front Door Cisco Prime Service Catalog URL	https://scdev/RequestCenter/
Admin Cisco Prime Service Catalog 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	

Category	Site Name/Usage (for example, Dev)
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
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
WebLogic	
Console URL	
User/Password	
Node Name(s)	

Category	Site Name/Usage (for example, Dev)
Application Server	RequestCenter
Virtual host	requestcenter_host
Service Catalog	
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	
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

Category	Site Name/Usage (for example, Dev)
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

Category	Site Name/Usage (for example, Dev)
Service tables	50
Dictionary table pattern	DM_FDR_DICTIONARYTABLE_
Service table pattern	DM_FDR_SERVICETABLE_
Field pattern	FIELD
Dictionary Text type fields	40
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
LDAP	

Category	Site Name/Usage (for example, Dev)
Server Type	
LDAP Authentication	Simple
SASL Mechanism	—
BindDN	
BindDN Password	
Connection Mechanism	Non-SSL
SSL Type	—
LDAP Host	
Connection Port	389
Secure Port	—
LDAP User BaseDN	
Optional LDAP filter	

C H A P T E R **3**

Managing Content Deployment

This chapter contains the following topics:

Managing Content Deployment

Overview

You can use Catalog Deployer for content deployment and configuration management, for service designers, catalog publishers, finance administrators, and organization building resources to migrate application entities between development, test, and production sites.

Catalog Deployer provides customers with a change management process and history, allowing for reliable control over content changes, and changes to the organizational entities used by all modules of Service Catalog.

Catalog Deployer also supports the deployment of preconfigured services packaged within a branded content library by Cisco. Such services can be used as-is or as the templates for customizing the service definition to the organization's requirements, significantly reducing the time and effort required to implement actionable service catalogs.

Content Deployment using Catalog Deployer

Catalog Deployer offers two methods of content deployment.

- Source sites can use Catalog Deployer to extract or assemble a package of service definitions and entities for transmission to, and deployment on, a target site. In this case, all operations can be performed within the Catalog Deployer module, and there is no need for external programs.

- Alternatively, a package can be produced for export. Exported files are imported via Catalog Deployer into the target site's instance of Service Catalog. Since these are XML files, in text format, they can also be stored in a configuration management or source code control system. Branded content libraries are delivered in the form of an export file, so standard Catalog Deployer facilities may be used to import and deploy services available in the library.

Like all other Service Catalog modules, Catalog Deployer can be permissioned for use. Users may have abilities to view deployment history; to create and assemble a package for deployment; to import or deploy a package to a particular site; or the combination of these capabilities that best fit the users' responsibilities. All such capabilities may be assigned via standard roles or custom roles in Organization Designer module.

Key Features and Functionality

Key features include:

- Simplicity of use via the user interface. Packages for deployment are created, and can be populated, transmitted to a target site, or exported to the file system.

- Two methods of content transfer: XML package transmission across sites or file-based transmission via export/import functionality.

- Service deployment (inclusive of related entities) on one or more target sites.

- Organizational deployment (OUs, groups, queues, roles, people, functional positions) on target sites.

- Email template and Service Link agent deployment on the target sites.

- Change management support (optional segregation of duties between content developers/managers and catalog publishers).

- Hot deployment—the ability to deploy content while the application is available to users.

- Online options to view extraction and deployment history.

- Support of site protection levels and entity homes.

- Ability to preview a service definition before it is deployed to a target site from a branded content library.

Catalog Deployer may be used at the beginning of a Service Catalog effort to provide template content which can form the basis of a customized service catalog. In addition, Catalog Deployer may be used in the Build and Maintenance phases of a development effort, to promote tested content from development to other environments and to synchronize multiple environments.

Configuration Management

The following sections discuss capabilities relevant to using Catalog Deployer for release and configuration management:

- Application Roles and Capabilities, on page 78
- Configuring Catalog Deployer, on page 82
- Catalog Deployer Packages, on page 88
- Sample Deployment Scenarios, on page 102

Service Catalog and Portfolio Development

The following sections of this chapter discuss capabilities relevant to using Catalog Deployer to install Cisco content libraries to provide the basis for a service catalog and service portfolio:

- Catalog Deployer Packages, on page 88 (only the sections on importing and deploying content.)

Catalog Deployer Architecture

Catalog Deployer provides database-neutral data-transfer infrastructure and interfaces, organized around the logical entities found in the application. Examples of logical entities are Service Definitions, Data Dictionaries, People and Organizational Units. A complete listing is available later in this section. There is however limited support for custom content across different databases and application environments. See the Unsupported Entities, on page 77 for the list of entities not supported by Catalog Deployer.

An understanding of Implementation, Site, and Entity Home, described in Table 44: Key Terms, on page 112, is critical to the operation of Catalog Deployer.

In particular, Logical Entity Home Sites are an integral part of configuration management with Catalog Deployer. Though optional with Catalog Deployer, creating a system of Home sites for logical entities enables management of both the referential integrity of logical entities across sites, and the integrity of configuration information across sites.

The idea behind Logical Entity Home sites is that certain sites will have a more authoritative version of the data for a logical entity type than others. For example, for customers using their LDAP directories to authenticate and gather information about users, data on People and Organizational Units are most accurate on Production. Therefore, the Production site would be the Home site, the site of record, for the People and Organizational Units. If People can be created, or Organizational Units edited, on sites other than Production, deploying this data to other systems will get them out of sync with the system of record, and the quality of data across the implementation will degrade.

Thus, the application framework is designed to allow protection levels to be assigned to logical entities to keep users from modifying these entities on sites other than the entities' Home sites. The site administrator can choose how much protection to provide for logical entities by choosing one of the four settings, as described in Configuring Catalog Deployer, on page 82.

Catalog Deployer deploys permissions for entities as part of the entity. When permissions are removed from the entity in its Home site, the application does not retain deletion stubs (or a transaction log) that Catalog Deployer may use to replicate this removal. For example, when the permission to order a service is removed from an Organizational Unit on a Service Definition, Service Catalog does not retain this fact, it simply removes the permission data.

When you deploy a service whose permissions have been changed, all associations between the service definition and its permissions are dropped in the target site and recreated according to the permissions in effect in the source site. However, if the permission was granted to a custom role or group, and the role or group was deleted from the source site, the role or group still exists in the target site. Catalog Deployer cannot propagate entity deletions.

Supported and Unsupported Entities for Catalog Deployer

The following table lists all logical entities supported for Catalog Deployer and their associated application module.

Table 35: Supported/Unsupported entities

Module	Supported Entities
Service Designer	Service definitions (Offer, Form, Form Sections, Plan, Authorizations, Permissions) Component entities automatically deployed with service definitions: • Service Groups • Dictionaries and Dictionary Groups • Active Form Components and Component Groups • Keywords, Categories, and Presentation Elements • Script Functions and Libraries Entities referenced by service definitions: • Email Templates • Organization Designer entities • Service Link agents and transformations
Service Item Manager	Component entities automatically deployed with service definitions: • Service Items (if referenced by a Service Item-Based Dictionary or by a table-based data retrieval rule) • Standards (if referenced by a table-based data retrieval rule) Service Items and Standards can also be deployed separately.
Service Link	• Agents • Transformations associated with the chosen agent are also deployed.

Module	Supported Entities
Organization Designer	• Queues • Organizational Units • Groups • Roles • Functional Positions • People
Administration	• Email Templates • Target Type allows you to export stack components for Infrastructure/Application templates into a new environment. Target Type is displayed by default in custom packages.
Demand Management	• Account Definition • Agreement Templates • Billing Rates

Catalog Deployer copies the entities listed above from the source site database to the target site database. Catalog Deployer does not move or copy information stored in the file system. Catalog Deployer copies the definition of libraries associated with JavaScript functions.

Unsupported Entities

Catalog Deployer migrates logical entities which are stored in the transactional database between two sites which are implemented using the same version of Service Catalog. The entities are extracted to a text stream, formatted in .xml, which is part of a deployment package which also includes the specifications (options) used to create the package. That package may be extracted from the source database, to serve as a backup mechanism as well as the source for deploying the entity definitions into the target database of another site. The entity definitions are deployed unchanged into the target environment.

> **Note** Catalog Deployer **does not support** deploying images (presentation elements) in .bmp format. Service Designer now prevents such images from being specified. Any legacy images should be converted to an alternate format, such as .jpg or .gif, optimized for presentation on the web.

Catalog Deployer has no effect on any components of Service Catalog other than those logical entities. Changes to some of these components are not part of the configuration management scenario handled by Service Link—the synchronization of customer-designed and configured configuration items across an implementation—so need not be considered further here. For example:

- Software components must be installed and configured via the Service Catalog Installer.

- The contents of the data mart and reporting tables must be created via Service Catalog Installer and populated via Extract-Transform-Load (ETL) processes.

- The schema is upgraded as part of the Service Catalog installation.

- Any customized Service Catalog components, or additional components, need to be installed on all servers via the "Customizations" option in the Service Catalog Installer and the procedures documented in this guide. Such customizations typically include support for custom mappings used in directory integrations, and any APIs provided by the Advanced Services organization.

However, additional configuration items may have to be deployed in conjunction with changes to the logical entities which are handled by Catalog Deployer. These are summarized in the following table and discussed in more detail in conjunction with the logical entity affected.

Table 36: Not supported entities

Configuration Item	Additional Artifacts to be Controlled and Migrated
External Dictionary	DML and DDL scripts run in the database
Datasource	Datasource specification to reference an external dictionary, a SQL-based option list or a table referenced in a data retrieval rule
Data Retrieval Rules	SQL Statement directly entered into the rules (may not be compatible across different database types)
ISF Script Library	Library (JavaScript) text file deployed on the application server
Custom Adapter	Deployment file produced by the Service Link Adapter Development Kit (ADK)

Application Roles and Capabilities

The key roles are defined as follows.

Table 37: Key Roles

Role	Definition
Catalog Publisher	Creates and maintains service catalogs and is responsible for deploying catalog content to the runtime application, configuring the look and feel and structure of catalogs, and for updating the deployed catalog content on an ongoing basis as the service definitions and delivery plans change.

Role	Definition
Service Designer	Designs service definitions at a customer site. Service designers have significant subject matter knowledge of the services provided to the customers of the customer IT team, and are proficient in the usage of Service Designer and Organization Designer. Services designers should be moderately technical, but are typically business analysts rather than engineers. Service designers may frequently need to create and modify service definitions within their development site. Some are allowed to use the Catalog Deployer for publishing their work to a staging or production site.
Organization Builder	Designs Organization Designer organizational entities at a customer site. Organization builders have significant subject matter knowledge of the organization's needs with regard to configuring the organizational units, groups, and roles necessary to successfully deploy and use Service Catalog. Organization builders should be proficient in the use of the Organization Designer module. Organization builders do not need to be highly technical, but should be an application administration IT resource.
Site Administrator	Performs application permission administration at a customer site. This person may be the first user of the system and is able to access all facets of the back end of the application, such as setting Global Configurations; managing lists such as languages and billing categories.
Change Manager	Approves change requests for the implementation at a customer site. This person is typically responsible for the stability of the production site and needs to understand all changes prior to their deployment to the production site. This role is optional, but is required in those customer sites that have established formal change control processes.
Service Administrator	Creates and manages UCSD, CloudCenter, and UCS PM integrations. This person is also responsible for creating and mapping custom templates for the UCSD services and CloudCenter applications. Service Administrator has access to the following modules: Service Catalog, Service Designer, Order Management, Administration-Manage Connections, and Integrations.
Team Administrator	Creates and manages teams. The team admin can view the servers, deployments, and order management related to all the users of that teams and the associated sub teams. Team admin has permissions to create/update/delete sub teams and modify the parent team for them. This person can also view all the teams and users down the hierarchy irrespective of who created the sub-teams.

The following table describes the system-defined roles along with the default capabilities granted to each role, relevant to the Catalog Deployer module.

Table 38: Predefined Roles and Capabilities

Predefined Roles	Capability					
	Manage Basic Service Deployments	Manage Advanced Service Deployments	Manage Custom Deployments	Import Deployments	Deploy Deployment Packages	Package Branded Content Libraries
Catalog Designer and Administrator	✓	✓	✓			
Organization Designer			✓			
Site Administrator	✓	✓	✓	✓	**P**	✓
Catalog Publisher	✓	✓	✓	✓	✓	
Licensed Content Publisher	✓	✓	✓	✓	✓	✓

Service Catalog Implementation and Configuration Management

This section describes how to design a Service Catalog implementation and the associated processes that support industry-standard configuration (or change) management practices.

Typical methodologies are reviewed and compared with those available for Service Catalog applications, including Catalog Deployer configuration management. The section discusses different approaches to configuration management, as they are matched to the stage of deployment—from initial development, through testing, deployment, and maintenance.

Catalog Deployer Best Practices

Catalog Deployer implements best practices embodied by IT industry standard configuration management methodologies and technologies. Therefore, it is useful to review these practices.

- Changes to software configuration items (that is, the individual software modules or components that comprise the IT application) are made in a development environment.

- In the same (development) environment, the changed software typically undergoes preliminary testing (unit testing).

- Once the software has passed unit tests, a copy of the "source" for the software is checked into a source code control system and labeled as the release candidate. "Source" may consist of several types of artifacts, including code written and maintained in a text editor, or, increasingly common, specifications stored in XML files or within a metadata repository that is part of an integrated development environment.

- The saved source is deployed to a tightly controlled test environment, where it undergoes rigorous testing. The test environment may be reinitialized before each set of tests, to ensure that results in different runs are comparable.

- The testers are responsible for finding problems, not diagnosing or fixing them. All problems are reported to the development team, which uses its development environment to fix the problems, retest the code, and save a copy of the revised source.

- The fix, extract, deploy, and test steps are repeated until the testing team certifies that the software meets all test criteria—these may be performance measures or functional requirements or a combination.

- The same source that was deployed to the testing environment (and tested!) is deployed to the production environment.

Configuration Management

For Service Catalog applications, the software that is developed is typically a service definition with related elements such as categories, groups, tasks, and checklists.

Catalog Deployer can be used by customers to deploy content such as service definitions, as well as any associated services.

The typical configuration management scenario, and the role that Catalog Deployer plays is similar to the following:

- A new or enhanced service definition is developed and unit tested in a development environment.

- Catalog Deployer is used to extract the new or updated service definition from the development environment. The resultant deployment package may be exported and placed under source code control if desired.

- Any other code resources (such as JavaScript libraries) that do not reside in the Service Catalog database may also be placed under source code control.

- Catalog Deployer is used to deploy the service definition in a test or quality assurance (QA) environment.

- The service is tested. If problems are encountered, the previous steps are repeated—code is fixed in development, extracted, and redeployed to the test environment—until the service is certified as having met the stated requirements.

- Once the service is accepted in the Test environment, it is deployed to the production environment, using the same procedure that originally deployed the code to the test environment.

This scenario adheres to industry standards in that the development environment is the only place changes are made to the service definition, and an automated process is used to deploy a controlled set of source code to test and production environments.

However, this scenario is incomplete. In most implementations, people and business units (a type of organization) are dynamically added to the Production environment, as people log in to Service Catalog for the first time, have a service ordered on their behalf, or are assigned to perform a review or authorization. Therefore, Catalog Deployer must also be used to migrate these entities from the production site back to

development, so they are available for use in service definitions and other Service Catalog configuration items, such as authorizations, that are still under development. Further, the service definition may refer to related entities such as email templates, groups, queues, service team-organizations, and roles. If any of these do not exist in the target environment, they must be deployed to that environment before the service's deployment package can successfully be deployed.

Configuring Catalog Deployer

Configuring Catalog Deployer involves:

1. Meeting the prerequisites for installing Service Catalog and configuring client workstations to support Catalog Deployer.
2. Installing a version of Service Catalog that includes Catalog Deployer. Catalog Deployer is automatically installed as part of all Service Catalog sites.

Note All sites including service packs should have the same version of Service Catalog.

3. Configuring implementations and sites within the development and production Service Catalog instances.
4. Configuring application server JDBC data sources on source and target sites.
5. Using the Administration and Organization Designer modules to ensure that personnel have access to Catalog Deployer capabilities appropriate to their functions in the implementation.

Note Passwords for 'Persons' and 'Agents' data imported from a different database (using Catalog Deployer or REX), must be reset in the target database. This is because the Key Encryption Key is different for different instances of Prime Service Catalog databases. If the passwords for 'Persons' and 'Agents' are not reset, they cannot be decrypted correctly in the target database.

Configuring Client Workstations

The deployment package produced by Catalog Deployer contains a compressed XML representation of the definitions of the included entities. Catalog Deployer uses file-based transmission of packages, in which package contents are transferred from one site to another via the export of the package and its subsequent import into the target site.

To support this file-based transmission, the user's browser must be configured to allow encrypted pages to be saved to disk. To do so:

Step 1   Choose **Tools** > **Internet Options** > **Advanced**.

Step 2   Click **Do Not Save Encrypted Package to Disk** check box.

Step 3   Click **Ok**.

✎

| **Note** | This configuration is not required if all deployments are via direct site-to-site transmission. |

Configuring Implementations and Sites

Before using Catalog Deployer, you need to use the development and production instances to configure your implementations. An implementation is the collection of sites among which Catalog Deployer migrates Service Catalog service definitions and other Service Catalog entities.

Configuring implementations and sites consists of the steps summarized below, also described in detail in the following section:

Step 1   Assign a name to the implementation. This name typically reflects the company or the project. This name is for documentation only, and is not used by Catalog Deployer.

Step 2   Name the Sites within the Implementation.
Within an implementation, each site must have a unique name. Service Catalog uses this name to identify the site for purposes of assigning protection levels for the Service Designer and Organization Designer pages that allow users to change (add, modify, and delete) entities.

Two sites are typically required: Development (DEV) and Production (PROD). Additional sites, for example, STAGE, TEST, or QA, may be used if configuration management and migration plans call for their use.

Step 3   Specify the Home Site for Each Logical Entity:
Specify the (single) Home site for each logical entity. A few rules are useful in making a decision about the Home sites for logical entities:

- A logical entity should typically be Home at one and only one site. This will allow you to better manage changes to the entity instances.

- Any logical entity involved in the definition of a service should clearly be home in the development instance.

- Any logical entity created through production use of the system should be Home at the Production site. If Single Sign-On (SSO) or Directory Integration which includes an Import Person event is enabled, logical entities home in Production will include people (and thus queues, as they are in the same table). If the automated user creation facility creates Organizational Units, then Organizational Units should also be Home at the production site.

| **Note** | Logical entities are almost never Home at a test or stage site. This is because such sites are typically rebuilt with production data and newly developed code to be tested. |

Step 4   Create a Data Source for Each Site
For Catalog Deployer to deploy content to a site, a JDBC data source must be configured for that site in the application server running the Service Catalog application. For example, in order to deploy services developed on the development site to test and production, the development site must include data sources for both the production and test sites; to deploy organizational entities from the production site to development, the production instance must include a data source for the development instance.

For clustered sites, the data source must be accessible to each node that comprises the site.

Step 5   Repeat the Process for Each Site
The data that specifies implementations, sites, and logical entities is, in turn, stored within logical entities.

These specifications must exist in all Service Catalog instances which comprise the implementation.

You also need to create appropriate data sources at all sites.

Configuring Implementations in the Administration Module

You must configure your implementation environment settings in the Administration module to begin using Catalog Deployer. The values you set in Administration allow source sites to recognize target sites.

These steps must be performed after you have defined your data sources in the JDBC data source page on the application server console.

To configure an implementation:

Step 1 Log in to the development instance as a user with Administration privileges.

Step 2 From the module drop-down menu, choose **Administration**.

Step 3 Click the **Settings** tab.

Step 4 From the menu on the right-hand side, choose **Entity Homes**.
The Logical Entity Home Specification page appears.

These settings influence the behavior of Catalog Deployer as well as the Service Designer and Organization Designer modules. If they are set improperly, incorrect data could be written to Service Catalog application sites, including production. Only systems administrators should change these settings.

Step 5 In the **Implementation Sites** section, in the text field at the bottom of the page, enter a site name; for example, "Development".

Step 6 From the **Select a Data Source** drop-down menu, choose a data source and click **Add New**.
The site name is added to the list of site names.

Step 7 Add the name for your production site as another site.

Step 8 If the implementation includes other sites which need to be refreshed via Catalog Deployer, such as QA or Test, add these as well.

Step 9 At the top of the page, in the **Implementation Name** field, enter an implementation name; for example, **My Cloud** or **Data Center Management**.

Step 10 From the **This Site is** drop-down menu, choose the development site to identify the current site and click **Update**.

Step 11 Review the **Home Site** assignments for the entities, changing any that do not fit your requirements. Click **Update** when finished.

Step 12 Assign the appropriate **Site Protection Level** to each site you have defined. Click **Update** when finished. These protection levels alter the behavior of the Service Designer, Organization Designer, and Administration pages through which the corresponding logical entity is maintained.

Table 39: Protection levels

Protection Level	Effect on User Interface at Nonhome Sites
None	Nothing: all UI elements for creating and modifying entities remain available. A protection level of "none" should only be used on a development site, in the initial phases of an implementation. This allows all entities to be created, modified, or deleted within the site by users who have appropriate roles.
Create only	Controls for creating new logical entities are disabled.
Create, Modify	Controls for creating and updating logical entities are disabled.
Create, Modify, Delete	All controls for creating, editing and deleting logical entities are disabled. A protection level of "Create, Modify, Delete" should typically be applied to any test, staging, or QA sites. These sites would typically be refreshed by copying a complete database from production (for example, to support performance or volume testing) or by deploying services from development for functional testing prior to promotion to production. A protection level of "Create, Modify, Delete" should typically be applied to the production site. A protection level of "Create only" would allow minor modifications to be applied to protected entities, such as changing an entity name.

Note   The same site names, entity home settings, and protection levels should be specified at all sites in an implementation. This will prevent users from inadvertently creating or modifying an entity at the wrong site, where it could be overwritten by the next deployment of the "same" entity, developed and maintained at a different site.

Configuring Data Sources for Sites

In order for Catalog Deployer to transmit a package to another site, the JDBC data source that corresponds to the target site must be configured in the same application server as the source site. The procedures for configuring the JDBC data source are the same as those for configuring the RequestCenter data source, as outlined in the Cisco Prime Service Catalog Installation and Upgrade Guide.

The same JNDI name prefix should be used to allow Service Catalog to discover the data source. The list of discovered data sources appears in **Administration > Settings > Data Source Registry**.

Certain data sources are used for reporting purposes and are not meant to be seen by Service Designer and Catalog Deployer users. To limit the data sources to just the ones these users need, check the **Use for Entity Home Definition** check boxes for those data sources, and then click **Update**.

Configuring Sites

You would initially configure one site - you would typically start with the development site. The development site is the source site for service definitions that are migrated to other target sites that become visible to the source site. Any site can be configured as a source or a target site, or potentially both, depending on the configuration of your overall implementation.

For example, you might configure your development site to see your test and production sites, and configure the production site to see the development and test sites. In this scenario, you would deploy entities from development to test, and then from development to production, assuming that testing was successful. You would migrate organizational information from production to both test and development sites.

Repeat the configuration of potential target sites on all source sites, including the definition of required data sources.

To verify that configuration is successful, log in at each site, navigate to Catalog Deployer, and in the Action pane, transmit a package to one of the target sites you just configured by clicking **Transmit**.You should see your site in the drop-down menu as one of the target sites you can choose.

Figure 3: Target sites
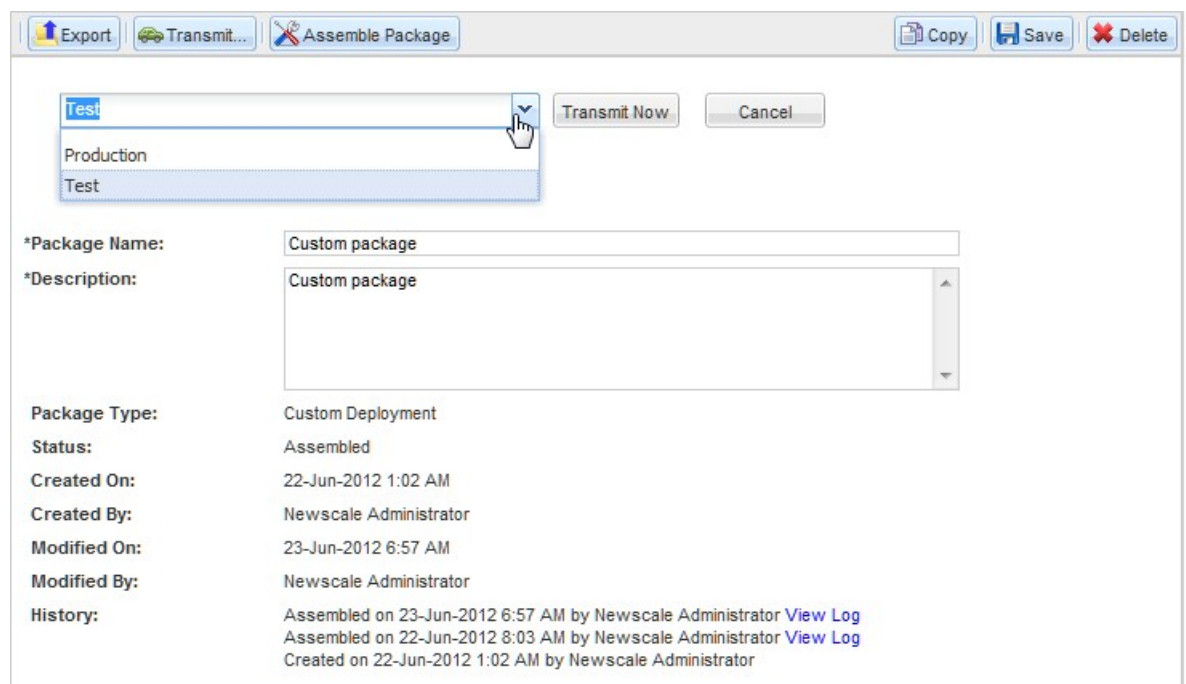
Catalog Deployer Performance Considerations

Catalog Deployer must be run when the source or target site is online and in use. However, it may be advisable to apply some restrictions to this usage.

Concurrent Usage of Catalog Deployer

Catalog Deployer consumes a significant amount of memory for assembling and deploying packages, as well as previewing services. To avoid any issues resulting from memory consumption, Catalog Deployer prevents more than five users from assembling, importing, or previewing a package at the same time. If a sixth user attempts to assemble, import, or preview a package, Catalog Deployer displays an alert to that effect, telling the user to try again later. While this may be an unlikely scenario in a Production environment, since the Production deployment will likely be handled by a single person, it may well occur in Development or Test environments if multiple service designers are packaging their respective content for deployment.

Browser Session Time-out

Package assembly or deployment is still considered interaction with the browser. Hence the session time-out for inactivity configured in the Administration module does not cause large package assembly or deployment to time out.

Package Size

Catalog Deployer only creates/updates associated entities a single time within a package if the entity is required for multiple primary entities. For example, if the "IT Software Configuration" dictionary is necessary for 20 services within a deployment package, Catalog Deployer only creates/updates the dictionary once on the target site. In grouping services with shared components in the same package, the size of the package and the number of redundant creations/updates Catalog Deployer must perform can be reduced.

Users can expect the performance of a large package (as defined by its size) to be slower. Users should also be aware that assembly or deployment of such packages may occasionally fail. If this occurs, the solution is to simply break the package up into a smaller set of primary entities; for example, creating two packages of 10 services each instead of one consisting of 20 services.

Hot Deployment

In principle, Catalog Deployer can deploy a complete package in one database transaction. In such a case, failure to deploy any one component (for example, a service definition in an advanced package cannot be deployed because a specified queue does not exist in the target) would result in the entire package contents being rolled back. The target site's repository would remain as it was before the deployment was started.

In practice, however, this all-or-nothing deployment may cause problems. Once an entity has been deployed, it is not available to online users until the complete package has been deployed and the database transaction committed. If, during this time frame, a user attempts to order a service that has been updated by the ongoing deployment, the user's session would hang, waiting for the service definition to be available. Eventually, the user would receive an error (worst case) or, after a delay, be able to order to service (best case). (This error may occur only when a user is initially ordering a service, not when task performers or authorizers are working with this service.)

One sure way to avoid this scenario is to not allow deployments while a production system is in use. This complies with the industry-accepted best practice of performing updates to a production system during a regularly scheduled maintenance window. However, waiting to deploy until a maintenance window roles around may not be possible. To minimize the probability of problems arising if a deployment must be run when Service Catalog is operational, it is advisable to group services into smaller logical packages. The service designer can still take advantage of reduced package size for shared components by grouping related services into the same package.

Catalog Deployer Packages

This section provides a general overview of Catalog Deployer functionality. The deployment package types—Basic Services, Advanced Services, and Custom—differ in the primary entities each can deploy and the options available for governing deployment of associated entities.

Basic Services Deployment Packages

Basic Services deployment packages work in a similar way as importing service definitions in Service Designer. If any associated entities (for example, a queue or organizational unit) are not found on the target site, the deployment would simply skip the entities not found. Basic packages cannot include bundled services.

Service deployment package also captures Standards and Service Items. The ones that are referenced in lookup Dynamic Data Retrieval (DDRs) and Service Item-based dictionaries are automatically included in the package. There is an Administration global setting that controls whether the standard entries are to be deployed as well (they are always captured; the control takes effect on deployment target only).

You can optionally control rendering of the blank/empty values fetched by DDRs as such on the service form, by setting the `serviceform.ddr.null.value.as.empty` property in the newscale.properties file to true.

As a default behavior, the basic services checks for the categories on the target site. If the source site categories exist on the target site, the services will be added to the associated category on the target site. If these categories does not exists on the target site, a new category will be created on the target site and will be merged with the source site entities.

Note   You do not need permissions in Service Designer to view and choose services for deployment in Catalog Deployer.

The content of a Basic Services deployment package and its associated entities are summarized below.

Table 40: Basic Service deployment package

Content Type	Action	Entity Types/Description
Primary Entity	Chosen via the Services content tab	Service Definition—All aspects of the service definition as defined in the Service Catalog option of Service Designer

Content Type	Action	Entity Types/Description
Component Entities	Automatically deployed	All entities referenced by the Service Definition: • Categories • Data Dictionaries • Dictionary Groups • Active Form Components • Active Form Component Groups • Keywords • Objectives • Presentation Elements • Script Functions • Script Libraries • Service Groups • Service Items and Service Item Groups • Standards and Standard Groups • Extensions
Associated Entities	Deployment will skip the entity association if any is not present in the target site	All entities referenced by the Service Definition: • Agents • Email Templates • Functional Positions • Groups • Organizational Units • People • Roles • Queues

By default, Catalog Deployer deploys Standards data as well as the Standard definition. You can override this behavior by disabling the Administration setting to **Deploy Entries (data) in Standards Tables**. You may wish to adopt this, for example, if a different set of data should be used in different environments or data is being provided via a file import from an external source.

Advanced Services Deployment Packages

An Advanced Services deployment package deploys the specified service definitions and their components. This package type provides the ability to control options for how to process the associated entities of a service definition during the deployment on the target site.

The Advanced Services deployment has two major differences from a Basic deployment:

- All services comprising a bundle can automatically be deployed by choosing the parent service and indicating it is a bundle.

- The user can specify which action to take if associated entities do not exist on the target site at the time of the deployment. This overrides the behavior of a Basic Services deployment, which automatically fails if any associated entity does not exist.

The options which govern behavior of Catalog Deployer in an Advanced Services deployment package with the associated entity or the associated category are summarized below.

Table 41: Advanced Services Deployment Package for Associated Entities

Associated Entities Options		
Entities	**Available Options**	**Result**
Service Accessories and Prerequisites	Skip	
	Fail	
Agent	Skip	Reference to the agent is removed from the delivery or authorization task
	Fail	Deployment fails
Email Template	Skip	Reference to the template is removed from the delivery or authorization task
	Fail	Deployment fails
Functional Position	Skip	Association to the functional position is removed; assignment is to the Default Service queue
	Fail	Deployment fails
Group	Skip	Association to the group is removed; assignment is to the Default Service queue
	Fail	Deployment fails

Associated Entities Options		
Entities	**Available Options**	**Result**
Organizational Unit	Skip	Assign the task to the Default Service Queue
	Fail	Deployment fails
People	Skip	Assign the task to the Default Service Queue
	Fail	Deployment fails
Queues	Skip	Assign the task to the Default Service Queue
	Fail	Deployment fails
Roles	Skip	Assign the task to the Default Service Queue
	Fail	Deployment fails

Table 42: Advanced Services deployment package for Associated Categories

Associated Category Options	Result
Update Category	This option will add or skip the associations for a category on the target site only if the category is present on the target site. If the category does not exists on the target site, the associations will be skipped.

Associated Category Options	Result

Include Categories	Using this option to include the source categories on the target site. This option will create the categories on the target system, if the categories are not present already.
	
	• **Merge**: Merge will merge the category and association on the target system with the category and association from the source system. For example, consider the Service (S1) with Category C1 in the source system, and same service S1 with another category (C2) in the target system. After merging, the target system will contain service S1 with both categories (C1 and C2). If the associated entities for a category does not exists on the target site, do one of the following:
	
	   ◦ Fail: Stop the deployment.
	
	   ◦ Skip: Skip the associated entities from the target system.
	
	• **Replace**: If a category already exists on a target system, the existing association of that category would be replaced by the associated entities from the source system.
	
	   ◦ Fail: Stop the deployment.
	
	   ◦ Skip: Skip the associated entities from the target system.
	
	• **Skip**: Retain the associated entities as is from the target system.

Since the Skip and Create (available only for selected entity types) options substantially change the definition of the service, they should be considered useful for "quick-and-dirty" deployments only. The service's form component would be transferred intact; however, potentially significant changes could be made to the delivery plan.

Custom Deployment Packages

Custom deployment packages allow you to choose entities individually and control options for how to process associated entities during deployment. Custom deployment is typically used for organizational entities, Functional Positions, Email Templates, such as People, Queues, Roles, Organizational Units, Agents, Services Items, Standards, Billing Rates, Account Definition, Agreement Templates, Categories, and groups.

In the customer deployment packages, you can choose to replace only certain attributes for a service on the target site rather than replacing the complete service definition . Under the **Service Deployment** options , select the options that can be updated on the target site.

There are more granular options controlling Service Items and Standards deployment behavior. The Service Item instances and Standards entries can be optionally included as a part of the deployment. But the option

applies to all Service Item types and Standard in the package. To include entries for some Standards or Service Items but not the others, you will have to break them into separate packages.

During import, if the Unit rate flag is set (Source XML) in **Demand Management > Billing Rate> Billing Rate Definition,** the 'Merge' option is selected for Billing rates when creating the custom package in Catalog Deployer. If the rate table already exists in target, the 'Merge' option will be ignored and behaves as an 'Overwrite' by deleting the existing data records in the target.

The following validations should be in place for a Rate table which has 'Unit Rate' flag set. This should also be implemented for Demand Mgmt, NSAPI and REX flows.

- Only one attribute should be Billable.

- Only one data record should exist in the Rate table Data.

- The single billable attribute must be of the data type 'Number' only (Integer/Long/Double/Money).

- If there are multiple records in the data tab, do not allow the user to check 'Unit Rate' flag in the first tab.

Deploying categories via a custom deployment allows you to recreate all or part of the category structure of the source site in the target site. Chosen categories and their subcategories are deployed, and the relationship of the categories to services with which they are associated is re-established to match that in the source site. This supplements the capabilities provided by Basic deployment packages, where only those categories associated with the services being deployed are included in the package.

While deploying a category on the target side, you can choose to :

- Not include the source side association and retain only the target site entities.

- Or include the source side association and merge/replace/skip the target associations in case the category already exists on the target site.

A package may contain more than one type of entity where there are interdependencies between the entities. For example, a person must be associated with an existing organization. Catalog Deployer automatically deploys entities in the correct order, so these interdependencies may be maintained.

Further, there may be interdependencies among entities of the same type: a person may designate another person as a supervisor, or an organizational hierarchy may exist. In these cases, Catalog Deployer also deploys entities in the correct order (the supervisor entity first, for example) so the relationships may be re-established.

For each of the entities (except functional positions) to be deployed, you have an option to overwrite the entity definition at the target site with the new definition contained in the package, or to skip the deployment.

Skipping entity deployment is risky since Catalog Deployer only checks for the existence of the entity in the target site, and does not inspect its content (for example, to see if the source is newer than the target). The Skip option can optimize performance by not reinstalling entities that already exist, but should be used in limited circumstances (for example, if you are deploying a large package for the first time into a target site where the entities are not known to exist). If any aspect of the deployment fails (for example, you attempt to deploy a person whose home OU is not in the target site and not in the current deployment package), you can fix the omission and redeploy the package. Only package contents that still do not exist in the target site would be deployed.

For each entity type (except email templates, functional positions, and agents), you also have the option to specify the behavior of Catalog Deployer with regards to re-establishing relationships to other related entities in the target site.

- Use "Do not include" to deploy only changes to the entity definition, without attempting to duplicate the relationships in the source site. This would be required if, for example, you want to deploy a new organization only, and not the relationships of this organization to numerous people, some of whom might not exist in the target site.

- Including source site associations will typically be required. This will duplicate the relationships in the source site at the target site. Using the "Skip" option will allow the deployment to continue if some of the associated entities are not present in the target site. For example, you may have assigned a queue to a service that is still in development and has not yet been deployed. If you use the "Skip" option, be sure to read the logs carefully, to ensure that no expected associations have been skipped.

You can also merge data imported from source site to target site during deployment. This option is available for service item definitions, standard definitions, billing rate definitions, and agreement templates.

Note Portal page and portlet permissions can be deployed with roles. The deployment must be performed after the portal pages and portlets have been imported through Portal Designer.

Creating and Deploying a Deployment Package

A deployment package follows this flow in Catalog Deployer:

Step 1 Create a Deployment Package. Persons granted permission to access and use Catalog Deployer can create a deployment package and choose the entities to be included in the package. See the Creating a Deployment Package, on page 95.

Step 2 Assemble the Package. When the underlying content is considered ready for deployment, a deployment package is assembled by clicking **Assemble Package** in the Action pane. At this time, Catalog Deployer extracts the content and creates a copy saved as part of the deployment package. Once package assembly has occurred, any changes to the entities included in the package are not captured unless the package is reassembled. See the Assembling a Deployment Package, on page 96.

Step 3 Transmit the Package. The assembled package is sent to a target site for deployment. Packages may be transmitted via Catalog Deployer, or, if there is no direct connectivity between source and target sites, you may perform this step "off-line" using the export and import process. See the Transmitting a Deployment Package, on page 96.

Step 4 Deploy the Package. A person with permission to deploy the package selects the received package on the target site and runs the deployment. See the Deploying a Package, on page 98.

Step 5 View Record Log files record all activity that occurs within Catalog Deployer on each site. See the Log Files, on page 101.

Step 6 For entities that are not supported during deployment, see Unsupported Entities, on page 77

Note It is only necessary to save packages when the package definition is modified. Package content is automatically saved.

Creating a Deployment Package

To create a deployment package:

Step 1   Choose **Action** > **New Deployment Package** in the View and Search pane.

Step 2   Enter the following details in the New Deployment Package window:

- Package Name

- Description

- Package Type

Step 3   Click **Save**.

Note
- Standards for naming packages should be developed, to allow users to infer the package contents from its name. For example, the name could consist of a designation of the type of package, the source site, a description of the content, and the build number or date the package was created. You cannot create two packages with the same name in the source or target site.

- The application will not allow the user to enter Package Names that use special characters (for example, no "\ /:*?"<>()[]" and so on). Spaces are allowed, but they are replaced with an underscore (_) in the Log XML Output file.

- Package description is required. Both the package name and description can be modified after the package has been created.

- If needed, click the package name in the View and Search or Content pane to see the Package Name and Description fields. The search results only return packages where the entity type or search value entered were primary entities within the package. Primary entities are those entities (service definitions, organizational units, groups, queues, people, functional positions, roles, categories or email templates) that were chosen for inclusion in the package

- The Package Type cannot be changed once the package has been created. See the Log Files, on page 101 for more information on Package Types.

Adding Content to a Deployment Package

When a package is created, it is assigned a status of "Not Transmitted". When it is clicked in the View and Search pane, its contents appears in the Content pane.

To add content to a package:

Step 1   In the Content pane, click the **Add** drop-down menu and choose the type of entity you wish to add from the list of available entities for that type of package.

A Search dialog box appears where you can search for and choose content.

Step 2 Choose the content you want by checking its check box.

Step 3 Click **Add** to add the chosen content.

The content appears in the Content pane and is automatically saved. If you need to remove an entity, check its check box, click **Remove** and then **Yes**. Content may be added and removed at any time until the package has been transmitted. If content is changed after the package has been assembled, the package must be reassembled.

Previewing Package Contents

Basic and Advanced Services Deployment Packages allow you to preview the definition of a service.

For a service that is already been included in a package:

go to the Content pane of the Package, choose the service to be previewed by checking its check box, and click **Preview**.

A service preview consists of a summary of the service definition, as well as a rendering of the service form. All entity references are summarized in the "Additional Content" section at the end of the preview. This may help you ensure that these entities are present in the target environment before you deploy the service.

Assembling a Deployment Package

In the Action pane, click **Assemble Package** to assemble a package. Click **OK** to confirm that package assembly was successful. Once a package has been assembled, its status remains "Not Transmitted". It can be reassembled if the definition of any of its components changes, or if you want to add or delete entities to be deployed. The log entry for package assembly includes both the primary entities specified and any component entities that will also be deployed. In the History section of the Action pane, the log may be viewed by clicking the **View Log** link.

Transmitting a Deployment Package

Content can be transmitted directly to another site if:

- The target site has been defined in **Administration > Settings > Entity Homes**.

- A datasource corresponding to the target site has been defined in the JDBC data source page on the application server console.

To transmit a package:

Step 1   In the View and Search pane, use the View drop-down menu to view packages with the status of: **Not Transmitted**.

Step 2   Locate the package within the list. Click the package name to view its information in the other panes.

Step 3   If the package has not been assembled, in the Action pane, click **Assemble Package**. Click **OK** to confirm that package assembly was successful.

Step 4   In the Action pane, click **Transmit**.

Step 5   Choose the target site from the drop-down menu.

       Note   You can choose only those data sources for which your site administrators have configured. See the Cisco Prime Service Catalog Designer Guide for instructions. In situations where no sites are listed, the site may be configured to only use the export/import functionality of Catalog Deployer.

Step 6   Click **Transmit Now**.

Step 7   Click **OK** to confirm that the transmission was successful.

    The deployment package is transmitted to the target site. The status of the current package in the source site is changed to "Transmitted". A transmitted package may be transmitted to additional sites or exported.

Exporting a Deployment Package

A package can be exported, instead of or in addition to being transmitted. Exporting a package produces an XML file consisting of the content of the assembled package. The export file can then be imported into a target site and deployed.

Exporting a package provides a textual representation of the package. It can be used as offline archival or checked into a corporate source code control system.

To export a package:

Step 1   In the View and Search pane, use the View drop-down menu to view packages with the status of: **Not Transmitted** or **Transmitted**.

       Note   Packages which have been received for deployment, or deployed, cannot be exported.

Step 2   Locate the package within the list. Click the package name to view its information in the other panes.

Step 3   If the package has not been assembled, in the Action pane, click **Assemble Package**. Click **OK** to confirm that package assembly was successful.

Step 4   In the Action pane, click **Export**.

    An export dialog box appears, as shown in the example below.

Step 5   In the dialog box, click the file name link (in the example above, the file name link is **Basic Service Package02**).

    A File Download dialog box appears.

Step 6   Click **Save**.

    A Save As dialog box appears.

Step 7   Rename the file if desired and choose your desired destination.

The destination would typically be on a shared drive, accessible to all users with Catalog Deployer capabilities. Standards for naming directories and structuring subdirectories should be established to facilitate tracking packages. For example, a new subdirectory could be created for all packages deployed as part of the same change request.

Step 8   Click **Save**.

Step 9   Click **Close** to close the export dialog box.

Export/import can be used instead of transmitting a package in cases where security or other concerns do not allow directly transmitting a package from the source to a target site. The results are identical—the package is created in the target site in the "Received for Deployment" status, and can then be deployed.

Importing a Deployment Package

An exported package needs to be imported into the target system.

To import a package:

Step 1   In the View and Search pane, choose **Action > Import**.
An import dialog box appears, asking you to browse for the file to be imported.

Step 2   Click **Browse**.

Step 3   Find and choose the package file.

Step 4   Click **Open**.

Step 5   Click **Import**.
The deployment package is imported, assigned a status of **Received for Deployment**, and opened. It can now be deployed.

Step 6   Close the import dialog box.

Note   To import a deployment package back into the source site from which it was originally exported, you must first delete the identical package from the source site. The application will recognize duplicate files even if the filename has been changed.

Deploying a Package

To deploy a package that has been transmitted to or imported into the target site:

Step 1   In the View and Search pane, use the View drop-down menu to view packages with the status of: **Received for Deployment**

Step 2   Locate the package within the list. Click the package name to view its information in the other panes
Note   The deployment runs according to the deployment options and associated entity rules that were chosen on the source site. Users at the target site can click through the tabs and view the entities chosen, but cannot modify the package in any way.

Step 3   In the Action pane, click **Deploy**

Step 4   Click **OK** to confirm that deployment was successful.

After the deployment completes successfully, the status of the package changes to "Deployed".

The assembled content of the package to be deployed must match the release level of the target site. Catalog Deployer tracks the application version under which the package was assembled, and will not allow deployment across different versions.

A Basic or Advanced Services package includes all the component design elements used by the services deployed. However, design components which are not stored in the database are not included in the deployment package and must be deployed separately. These elements include:

- JavaScript libraries referenced by any ISF Scripts

- Data sources added to the environment and referenced by data retrieval rules or option lists

In principle, deployment does not affect the service and component definitions used by requests that were in-flight when the deployment occurred. However, because of the dynamic nature of the requisition process, previously submitted requests are affected by:

- Changes to the content of rules or JavaScript functions and libraries

- Changes to the delivery plan of service requests that have not yet passed their final approval step

The deployment schedule and service designers need to take into account that in-flight requests based on the previous version of the service definition are affected by changes to the above elements.

Transmit and Deploy Multiple Packages

You may transmit and deploy multiple packages in one function. Catalog Deployer processes each package in turn, and provides the status for each. This procedure makes it much easier to deploy a large number of packages with limited user intervention.

To transmit multiple packages:

Step 1   In the View and Search pane, choose **Action** > **Transmit Multiple Packages**.

Step 2   Click **Add Packages to Transmit** to open a Search dialog box where you can search for and choose packages to be transmitted. The Search dialog box only allows you to choose packages with a status of "Not Transmitted" (which have been assembled) and "Transmitted".

Step 3   Choose the packages you want by checking their check boxes.

Step 4   Click **Add** to add the chosen packages.
The packages appear below the Packages folder in alphabetical order. All chosen packages are transmitted. If you need to remove a package, check its check box, click **Remove** and then **Yes**.

Step 5   Under the "Select a target site" folder, choose the target site by checking its check box.

Step 6   Click **Transmit** to start the transmission.
The packages are transmitted in the order in which they are listed (alphabetically). After the transmission process is complete, a status message appears, showing the transmission success or failure for each package. (The most common

reason for a transmission failure is a version mismatch between the source and target sites). The log file for each package is also updated.

Similar Interface to Deploy Multiple Packages

A similar interface is available to deploy multiple packages:

Step 1   In the View and Search pane, choose **Action** > **Deploy Multiple Packages**.

Step 2   Click **Add Packages to Deploy** in Deploy Multiple Packages window to open a Search dialog box where you can search for and choose packages to be deployed. Any package with a status of "Received for Deployment" or "Deployed" may be chosen.

Step 3   Choose the packages to be deployed by checking their check boxes.

Step 4   Click **Add** to add the chosen packages.
The packages appear below the Packages folder in alphabetical order. All chosen packages are deployed. If you need to remove a package, check its check box, click **Remove** and then **Yes**.

Step 5   Click **Deploy** to start the deployment.
The packages are deployed in the order in which they are listed (alphabetically). Like the multiple transmission, multiple deployment indicates the success or failure for the deployment of each package; that information is available in the package's log file as well.

Closing and Reopening a Deployment Package

A deployment package in any status can be closed in the site in which it was created by clicking it in the View and Search pane, and in the Action pane, clicking **Mark as Closed** Closing a package simply changes its status to "Closed", so that it appears only in the view of "Closed" packages, rather than in other views. This may make working with other packages easier, since there are fewer active packages to search through to find the one you want.

A closed package can be reopened at any time, for example, if you need to transmit it to another site or wish to export its contents. To reopen a package, click it in the View and Search pane, and in the Action pane, click **Reopen**.

Deleting a Deployment Package

To delete a package, click it in the View and Search pane, and in the Action pane, click **Delete**. Click **Yes** to confirm the deletion. Deleting a deployment package permanently removes the package and its deployment history from the current site. Although package contents are compressed, the XML required to represent the package components may be quite large. Therefore, deleting packages will recover usable space in the repository/database. Package contents could be recovered if the package was previously exported; however, the complete deployment history of the package at the current site could not be recovered.

Copying a Deployment Package

Unless you are very lucky, you will need to deploy the same entities multiple times as part of the build process. For example, you deploy one or more services from the development to the test environment; the testers find some defects that need to be repaired; the service definitions are repaired in development and redeployed, so that the fixes can be verified in test before being deployed to production.

The ability to Copy a deployment package facilitates this work flow. Once an initial package, with the desired content, is produced, you can copy the package.

To copy a package:

Step 1   Choose the package in the View and Search pane.

Step 2   In the Action pane, click **Copy**.
A Copy Package dialog box appears.

Step 3   Rename the package.

Step 4   Click **Copy Package**.

Step 5   Click **OK**.
The new package is created and opened with a status of **Not transmitted**—it contains the entities specified in the Content pane, not the assembled package content. You can then reassemble the package as required.

Log Files

The **View Log** link in the History section of the Action pane displays the actions by Catalog Deployer in detail. Clicking on the **View Log** link opens a View Log tab with Log Details and XML Output subtabs. Logs record all activity that a package undergoes. Assembly logs list all entities included in the package. Deployment logs list all entities successfully extracted on the target site. If the package failed to deploy, the error also appears.

Logs include all package details (name, description), time/date stamps for the time of assembly or deployment, and all included entities.

Known Errors and Omissions

Catalog Deployer does not support renaming entities. Catalog Deployer will not behave correctly if you rename an entity at the source site and attempt to deploy it or deploy a service that references the renamed entity. In order to establish (or reestablish) an association with a related entity, Catalog Deployer attempts to find the entity in the target site by name. For deployment purposes, an entity "name" is the name attribute of all entities except for people (identified by their login name) and organizations (identified by the combination of organization type and name). The result is that:

- For component entities of a service definition (dictionaries, form components), a new entity is created, and an association with this entity established for the service being deployed.

- For primary entities being deployed, a new entity, with the new name, is created.

- For associated (directory entities and email templates) entities, the deployment may fail or the entity association may be skipped, depending on the package type and deployment options chosen.

The workaround is to:

- Turn off site protection for the affected entities in the target site, if applicable.

- Rename the entity in the target site so the name matches that in the source site.

- Turn site protection back on.

- Deploy the entity.

During the development process, you should carefully track entity name changes, so they can be applied, as explained above, in the target sites before attempting to deploy the entity to those sites.

The unit of measures referenced in Objectives and Billing Rate Tables are not captured in the deployment packages. You should create any new unit of measures established for your services or billing rates through the Administration module in the target site before deploying packages that reference them.

Sample Deployment Scenarios

This section gives details on recommended procedures to use in some frequent development and deployment scenarios.

Initial Deployment

You need to create a new Service Catalog site. One option is to copy an existing Service Catalog database to the site, and adjust the installation and configuration to use that database. (The procedure for doing this is documented in this guidehttp://www.cisco.com/en/US/products/ps13206/prod_technical_reference_list.html .) However, another option is to perform initial configuration of the database and then use Catalog Deployer to deploy all entities that should populate the new site.

Performing Preliminary Configuration

Catalog Deployer does not deploy aspects of Service Catalog configuration that typically do not change as the Service Catalog evolves. Therefore, you must define these elements as you did for the initial site.

- Re-enter Administration modules settings for settings, directory integration, authorizations, and entity homes. These settings should be identical to those in Development except for environment-specific configuration items. (For example, you may have separate LDAP directories for Development and Test.)

- Ensure that any Service Link custom adapters were included in the installation procedure, and that any changes you made to Service Catalog adapters are reapplied.

> • Re-enter agents and transformations (a known error and omission).

Deploy Service Foundation Entities

Entities maintained via Organization Designer (people, organizations, groups, roles, and functional positions) must be present in a site before a service definition can refer to them. Therefore, all such entities must be deployed before the service catalog can be deployed. Such entities should be included in one or more Custom deployment packages.

In addition, any custom email templates must be deployed. Email templates can be deployed at any time before the service that uses them is deployed.

Deploy Services

Once the foundation entities have been deployed, services may be deployed. For the initial deployment, keep the package size manageable (say, group things by service group) and be sure to review the log carefully. A basic deployment should be used, since all associated entities should have been deployed earlier.

Placing Entities in Respective Servers

You should now have two (or more) sites in operation. All the services in Production should be identical to services in Development. (There may be additional services in Development that were part of the initial deployment, but that's okay.) In which environment will you be maintaining the entity definitions and membership (for groups, roles, and organizations)? In all cases, it is assumed that Entity Protection Levels are set to prevent any maintenance to entities in a non-home environment.

Directory-Related Entities Reside Only in Production

The most straightforward approach is to home all entities that comprise a service definition in the Development instance and to home all entities related to people and organizations in the Production instance.

This makes using Catalog Deployer and maintaining the entities it deploys very easy—all aspects of all entities are always maintained in one and only one site. However, it complicates the work flow for creating and testing directory-related entities.

1 Before developing a new service, take an inventory of the queues, organizations, groups, roles, and functional units that are referenced in the delivery plan or other areas of the service.
2 If all of these associated entities already exist in the Development instance, it means they already also exist in Production (since they are homed in Production). Therefore, you can proceed with creating and testing the service.
3 If any of these directory-related entities do not already exist, log in to the Production instance and create them. Configure the entity definition, as well as its membership and roles.
4 Logged in to Production, create a Custom Deployment package containing the new entities and its associated entities. The package will need to use the option to "Use Source associations" for the new entities, since there are not yet associations in the target instance.
5 Deploy the custom package into Development.
6 Create the service using the new entities just deployed.
7 When the service is ready to be tested, create a Basic Services package containing the service.
8 Deploy (in this order) the custom package containing the directory entities to the Test site. Then deploy the Basic Services package.

9 Once the service passes testing, deploy the same Basic Services package from Development to Production.

In this scenario, all work regarding the directory-related entities (except actually referring to them in a service definition) is done in one place, the Production environment. This is good, because all work is done in one place and is easy to review and monitor. However, this process does have the following potential disadvantages:

- You are probably adding steps to the development process: if you did not get the entity definitions correct the first (or second or third) time, you will have to go back to Production, fix the entities, repackage, redeploy and retest. When you repackage, you will need to use the option to "Use Target Associations" for the primary entity, since it has already been associated with a service that only exists on the target site.

- Another possible objection might be that you doing extensive development work in a Production environment, which some organizations see as a security risk.

Directory-Related Entities Reside in Both Production and Development

An alternate approach is to home all entities that comprise a service definition in the Development instance (this should never change) and to home entities related to people and organizations in both the Production and Development instances.

Homing entities such as organizations, groups, roles, and people in both instances has the following advantages:

- You can work on the definition of these entities in the logical place, the Development environment. It may take a few passes, for example, to get a custom role definition just right. You would not need to iteratively develop, deploy, and test—you could just develop and test, deploying when you are done.

- You can assign members to organizations or roles in the logical place, the Production environment, where all person information is automatically refreshed via directory integration and you are guaranteed that all Service Catalog users are represented.

Homing entities such as organizations, groups, roles, and people in both instances has the following disadvantages:

- Role-based access control currently allows access to a particular entity type. No further granularity is possible. For example, it is not possible to allow designers to define groups (and their roles) only in the Development environment, but only allow them to assign group membership in the Production environment.

- Since maintenance is happening in more than one environment, care must be taken when deploying packages. You must ensure that appropriate source and target associations to the entity are maintained.

As an example, assume you are developing a group whose members will consist of people across various service team organizations. The following section describes how to assign members to the group.

People and Groups Reside in both Production and Development

- Create the group in Development, and assign some (test) members in order to verify that the capabilities and permissions granted via the group are correct. Not all people who must be in the group are in the Development environment, so the member list is incomplete and potentially incompatible with people in production (if you have some "test" people who do not have corresponding entries in Production).

- Use a Custom Deployment Package to deploy the group to Production, using source associations, but skipping an association if the referenced entity does not exist.

- Using Organization Designer in Production, associate the appropriate people with the group. You may do this either via the People or Group pages, whichever is more convenient, since both entities are home in Production and the entities could be maintained even with a "Create, Delete, Modify" protection level.

- If membership in the group changes, you only need to go to Organization Designer in the Production environment and make the appropriate changes. Further, directory integration has the ability to dynamically specify a list of groups in which a person is a member; if this capability is enabled (via updates to the enterprise directory and a corresponding directory mapping) no manual updates would be necessary.

Deploying a Service to Use a New Queue

You need to develop a new service or enhance an existing service to use a new queue. Following best practices, the queue should have a corresponding service team organization in which it is homed.

There are two possible scenarios here, depending on where you have "homed" queues and organizations. Each has pluses and minuses. (This is just a special, and very frequent case of the discussion in the previous section.)

Organization Units and Queues Residing in Production

This is a "clean" approach that places all work on organizations, people, and queues in Production. It was the only workable approach in versions on Service Catalog prior to 2007, so people upgrading from those versions may prefer to keep using it.

- A disadvantage to this approach is that you are doing manual work in Production (creating queues and OUs), which some organizations may frown upon for security reasons.

- The advantage of this approach is that all work on the queues and OUs—not only defining them, but assigning their members —is done in one place.

- Create the OU and queue in Production and assign appropriate roles.

- In Production, assign members to the OU.

- Deploy the new OU and queue from Production to Development. Include in the deployment package all service performers in the OU. You may wish to set the People deployed to skip existing people, to optimize deployment performance.

- Create the service in Development.

- Deploy the service from Development to Production.

Organization Units and Queues Residing in Both Development and Production

In this scenarios consider that the definition of the entity is home in Development, but its membership is home in Production. (Of course, this division cannot be enforced by entity homes, so both sites are designated as home for the entities to allow maintenance via Organization Designer).

1 Create the OU and queue in Development and assign appropriate roles. Assign enough members so you can thorough test the new configuration.
2 Create the service in Development.
3 Deploy the new OU and queue from Development to Production, using source associations, but skipping any that do not exist at the target site (to exclude "Test" people).

4 Use Organization Designer (or rely on Directory Integration) in the Production site to assign members to the OU.

5 Deploy the service from Development to Production.

Maintaining Organization Units and Queues after Initial Deployment

In both scenarios above, you are faced with possible changes to the initial queue and OU configuration after initial deployment.

- Changes in membership in the OU are handled as for initial deployment, that is, the OU membership is maintained in Production. It is not critical that all such changes be deployed back to Development, but if this is desired, a Custom Deployment package of the OU and new or affected People can be produced and deployed to Development, using source associations.

- Changes in the permissions assigned to the OU are applied in the site where the entity definition is home. The new OU definition is then deployed to the other site, using target associations.

Deploying Services that use a New Email Template

Two packages are needed:

1 In Development, create a Custom package containing the email templates. Use the default deployment option—replace the existing entity.

2 In Development, create a Basic Services package containing the revised services.

3 Deploy the Custom package to Production.

4 Deploy the Basic Services package to Production.

Each package may be deployed as it is produced, provided the Custom package is deployed before the Basic Services package.

Renaming a Queue and Service Team

After several services have been deployed, which include tasks assigned to a particular queue, you receive feedback that the queue name is misleading to service performers, who would like it changed. Or perhaps the company has been restructured and organizations (including Service Teams) need to be renamed to reflect the new organization.

This runs smack up against a "Known Error and Omission" documented in the Known Errors and Omissions, on page 101. Since Catalog Deployer works by matching the names of entities across sites, it cannot match an entity that has been renamed. In some cases (as documented above), Catalog Deployer does fail and reports an error. In other cases, however, Catalog Deployer will create a new entity in the target. In the case of a renamed queue, any services previously deployed would still use the old queue. Only services deployed after the queue was renamed and deployed would reference the new queue. This is clearly not the intent of the designer.

The only way to prevent this behavior is to put in place processes that carefully monitor and control entities that need to be renamed. The processes would vary slightly, depending on whether queues and organizations are homed solely in Production, or in both Production and Development, but both involve manually renaming (via Organization Designer) the entities in both sites.

You must consider the following scenarios:

Entities Reside in both Development and Production

1 In response to the requirement, the Organization Designer renames the queue and service team in the Development instance, through normal maintenance procedures.
2 An Administrator manually (via Organization Designer) renames the entities in the Production instance. Since the entities are homed in both instances, entity protection levels would normally allow this step.
3 Service Designers work on services using the renamed queues and service teams. Such services can be deployed through standard procedures.

Entities Reside Only in Production

1 In response to the requirement, the Organization Designer renames the queue and service team in the Production instance, through normal maintenance procedures.
2 An Administrator relaxes entity home protection levels in the Development instance. This is necessary, since no manual changes to queue definition or membership is typically allowed, since the entity is homed in Production.
3 The Organization Designer renames the entities in the Development site.
4 The Administrator turns entity protection levels back on after the changes have been applied.
5 Service Designers work on services using the renamed queues and service teams. Such services can be deployed through standard procedures.

Changing a Category and the Icon

Categories are deployed as component entities as part of a basic or advanced service deployment. This is an effective strategy when your main objective is to deploy a new or revised service definition and to ensure that the associated categorization is also deployed. However, using a services package is not effective when the category hierarchy or images associated with categories have changed.

A custom deployment package offers the option to deploy all or a portion of the category hierarchy, independent of any services that may reference that hierarchy. When the category structure is deployed to the target environment, Catalog Deployer automatically re-establishes the associations between each category and its services.

As always, the warning against simply renaming an entity, in this case, a category, applies. If a category no longer applies, you should delete its association to services and create a new, replacement category. The alternative is to rename the category in the source and all target instances:

1 The Catalog Designer renames the category in Development (where categories are home).
2 An Administrator turns off entity protection in the Production site.
3 The Catalog Designer renames the categories in the Production site.
4 The Administrator turns entity protection levels back on after the changes have been applied.
5 Service Designers work on services using the renamed categories. Such services can be deployed through standard procedures.

Renaming Entities after a Service Catalog Upgrade

Service Designers can recognize entities with distinctive names as having been produced by the upgrade process:

- Every service definition has a corresponding active form component. The name of the form component is: "UPGD: Form", followed by the service name.

- All form components are assigned to a form component group. The name of the group is: "UPGD: Form", followed by the name of the service group where the service definition corresponding to the form resides.

Service Designers will want to, at a minimum, rename the artifacts produced by the upgrade process, so the names are more user friendly. (They may also want to refactor the structure of the form components, to promote reuse, but that is another issue.) This is a "standard" Rename scenario:

1 The Service Designer renames the form component and form component group in Development (where these entities are home).
2 An Administrator turns off entity protection in the Production site.
3 The Catalog Designer renames the form component and group in the Production site.
4 The Administrator turns entity protection levels back on after the changes have been applied.
5 Service Designers work on services using the renamed form components. Such services can be deployed through standard procedures.

Adding a Custom Functional Position

You defined a Functional Position in Development (related to an OU) and specified the person holding that Functional Position for one or two organizations. You've changed the service in Development to route tasks to that Functional Position. How do you deploy the new and changed entities?

1 Create a Custom package in Development.
2 The Custom package contains the functional position you created and the people who are assigned to that position. The deployment option for the people is to use source associations.
3 Deploy the Custom package to Production.
4 Create a Basic Services package containing the revised service.
5 Deploy the Basic Services package to Production.

Deploying to an Environment with Browser Cache Enabled

If the Browser Cache setting is enabled in the Administration Settings, changes made to icons and embedded images in the service catalog presentation 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 this guide to increment the browser cache version.

Branded Content Libraries

Cisco distributes content in the form of Branded Content Libraries in certain product releases. Contact the Cisco Technical Assistance Center (TAC) if you want to find out the availability of such content libraries for the release you are using. Two types of library packages are available:

- Service Library, containing service definitions and their component entities

- Custom Library, containing entities associated with a Service Library

The services in these libraries offer models for commonly required services for End User Management, Access Management, Data Center Management and other areas. Library contents can be previewed and desired items

deployed to a development environment. This provides a head-start for designing, configuring, and customizing these services to enterprise requirements.

Custom libraries contain entities such as queues and service teams (organizations), which are referenced in a service. These libraries can optionally be installed in conjunction with the corresponding service library. If the Custom Library is deployed, the service will use the predefined references. If the custom library is not installed, the service will refer to the "Default Service Queue" or remove the reference, as appropriate. Service designers are responsible for completing the task (delivery) plan configuration.

Deploying a Branded Library

Typically, a site administrator is responsible for administering and deploying content from branded libraries. If desired, a custom role which includes the capability to Deploy Branded Content Libraries may be created. See the Structuring the Organization, on page 143 or *Online Help* for details on creating and assigning roles.

Use the following procedure to deploy branded libraries:

Step 1 Obtain the libraries. Libraries and corresponding user guides are available for download from the Cisco software site.

Step 2 Install the library. The library must be installed on a directory accessible to the client workstation from which Catalog Deployer is run. A shared network drive will allow central storage of libraries.

Step 3 Ensure that users responsible for deploying library contents have roles that include this capability.

Step 4 Import the library. Import the library into Catalog Deployer. See the Importing a Library Package, on page 109.

Step 5 Review the library contents. A person with permission to deploy the library package selects the received package on the target site and optionally previews the library contents (services).
To preview library content, choose the service to be previewed by checking its check box, and then click **Preview**.

Step 6 Deploy chosen library contents. Choose the received package, choose the package contents to be deployed and run the deployment. See the Deploying a Library, on page 111.

Step 7 Review the deployment log. Deploying library contents generates a log detailing all deployment activities in regards to creating or updating entity definitions.

Site Administrator and Catalog Publisher roles include the Import Deployments and Deploy Deployment Package capabilities in order to import, preview or deploy content from Branded Content Libraries.

Importing a Library Package

Importing a library package is analogous to importing a deployment package:

Step 1 In the View and Search pane, choose **Action > Import**. (If that option is not available, the current user does not have a role that includes the "Deploy Branded Library Content" capability.)
An import dialog box appears, asking you to browse for the library file to be imported.

Step 2   Click **Browse**.

Step 3   Find and choose the library file.

Step 4   Click **Open**.

Step 5   Click **Import**.
The library is imported, assigned a status of "Received for Deployment", and opened.

Step 6   Close the import dialog box.

A library package has attributes which identify the library and guide you in its deployment:

Table 43: Import library package attributes

Attribute	Description
Package Name and Description	The name for the library and a brief description of its contents.
Library Version	The version of the library as released by the vendor.
Vendor Name	Cisco, or the name of the content provider.
Application Version	The version of the database for which deployment of the library is supported. Libraries are tailored to a specific version of Service Catalog.
Image	An image icon associated with the library.
Package Type	Service Library or Custom Library.
Status	The current status of the library. Either "Received" or "Deployed".
Created On/By Modified On/By	Catalog Deployer automatically tracks the person who created the library in this site (that is, who imported the library), and the date of the latest deployment activity and who performed it.
History	A brief log of all deployment activities performed against the library in this site with links to more detailed logs for deployment details.

Creating a Branded Library Package

Licensed users with appropriate roles can create a new library by choosing **Action > New Library Package** in the View and Search pane.

The procedure is identical to the procedure for creating a deployment package (see the Creating a Deployment Package, on page 95) with the following exceptions:

- **Library Version** and **Vendor Name** are required. These are free-format text fields which identify the library.

- An orange ball icon 🔴 is associated with a new library by default and is displayed in the first column of the View and Search pane. A custom image icon may be used by clicking **Upload Image** in the Action pane after the Library Package has been saved. Images can only be in JPG, PNG, or GIF format. They are displayed with a width of 16 pixels and a height of 16 pixels, so they should be created to maintain this aspect ratio. If the image is not sized correctly, it is resized by the browser and may appear blurry or pixilated.

- The Package Types available are:

  ◦ **Service Library**, containing service definitions and their component entities

  ◦ **Custom Library**, containing entities associated with a Service Library

- The library is also identified by the application version, the version of the Service Catalog database under which it was created. Libraries can only be deployed into a Service Catalog site running the same application version with which they were created.

- Library packages can only be exported, not transmitted. Just as for a deployment package, a library package must be assembled before export.

Deploying a Library

Libraries are the vehicles for new content to be distributed from Cisco to customer sites. A library should be deployed into a development site only. Catalog Deployer is designed so that libraries can be deployed without disrupting or overwriting existing content that may have previously been customized to the customer's requirements. Therefore, the options for deploying a library package are configured so that library contents can supplement, but not replace, any previously created content with the same name on the target site.

- Primary entities in the package (a service or directory-related entity in a Custom package) will only be deployed if an entity by the same name is not found on the target site. Deploying from a library never replaces existing content.

- A service bundle always includes the parent service definition as well as all child Service Definitions. As is the case for all primary entities, the service definition is skipped (not deployed) if a service with the same name already exists in the target site.

- Component Entities are entities that are automatically deployed along with a primary entity. For example, deploying a service entails deploying the dictionaries, active form components, categories, and keywords used by that service. Such component entities are not deployed if an entity with the same name already exists in the target site.

- Associated Entities are those entities referred to by the primary entity. For example, queues, peoples, and organizations can be referred to by a service task plan, and are the service's associated entity types. If an associate entity exists in the target site at the time the primary entity is deployed, a relationship is established between the entities. If the associated entity does not exist, a default relationship (for example, to the "Default Service Queue") is established.

The entire contents of a library containing supporting entities (such as queues and organizational units) must be deployed simultaneously. Conversely, Catalog Deployer allows you to choose the contents of a Service Library to be deployed. Each service is deployed in a separate transaction. If the deployment fails, the current transaction is rolled back.

All import and deployment actions are logged for the library package. The **View Log** link in the History section displays the actions by Catalog Deployer in detail. See the .

Terminology

Table 44: Key Terms

Term	Definition
Assemble a Package	Add content to a package. Assembling a package extracts the current definitions of the objects which have been included in the package from the repository and writes them to the package. Any subsequent changes to these objects will not be reflected in the assembled package.
Associated Entity	An entity that is related to the primary entity and required in the target site for a deployment to be successful. For example, a service definition (primary entity) may refer to several organizations, service teams to whom tasks are assigned (the organizational unit is the associated entity).
Catalog Deployer	The Service Catalog module responsible for deployment of catalog content and directory information from one site to another.
Component Entity	Entities that are automatically deployed when a service is deployed. Service component entities include categories, presentation elements, dictionaries, dictionary groups, service groups, keywords, and objectives.
Data Source	A data source, defined in the JDBC data source page on the application server console, which specifies connection information for all sites which become targets for Catalog Deployer direct site-to-site deployment.

Term	Definition
Deployment Package	The primary object managed by Catalog Deployer. The deployment package contains the chosen entities that are to be deployed (such as service definitions or queues and groups) and the deployment activity history. A deployment package can be transmitted or exported/imported into another site for deployment of its contents into the target site. A deployment package does not contain entity content until it is "assembled," at which point the included data is extracted from the source site.
Entity	One of the objects created and maintained within Service Catalog software. Examples are: organization units, service definitions, queues, and email templates.
Entity Home	The page of the Administration module's settings where administrators specify which site is the site of record for each supported entity type.
Export a Package	Create an XML file containing the contents of a previously assembled package and write the file to the file system. Exporting a package from a source site to a target site is an alternative to transmitting the package.
Implementation	A group of one or more Service Catalog sites, either directly or indirectly connected.
Import a Package	Create a package by importing a previously exported XML deployment package into a target site. The package is created with the status "Received for Deployment".
Library Package	A package from Cisco that has been preassembled and is available as a file import. The package content consists of template services or associated entities that can be used to provide the basis for a service catalog. Unlike deployment packages, chosen contents of a library can be deployed.
Primary Entity	An entity that can be chosen for inclusion in a Catalog Deployer package.
Site	A collection of one or many computer systems (single computer or cluster) that share a database and an http address, and can be categorized by function. For instance: a development site, a testing site, and a production site.

Term	Definition
Source Site	The site in which a package is created. This is the site which transmits or exports a package for deployment on another site.
Target Site	The site in which a package is deployed. This is the site which receives a package via transmission or import.
Transmit	Send a package from one site to another via a database connection. Once a job has been transmitted, it cannot be edited (reassembled and have its content changed) on the source site. The target site receives the transmission via Catalog Deployer.

Integrating with Cloud Applications

This chapter consist of the following topics:

Creating a Service Administrator

As a Site Administrator you can create a Service Administrator who is well aware of the UCS Director, CloudCenter and UCS PM applications. The Service Administrator role creates and manage UCSD, CloudCenter, and UCS PM integrations. This role is also responsible for creating and mapping custom templates for the UCSD services and CloudCenter applications.

The very first Service Administrator must be created by ordering the service **Create Service Administrator** from Service Catalog. Assign a person as Service Administrator from the Search for Recipient pop up and click **Submit**. This Service Administrator can then assign the same capabilities to others by ordering the **Create Service Administrator** service.

In case you have upgraded from previous version of Prime service Catalog and have already integrated with UCSD, then you must map the user who manages the integrations with the Service Administrator role.

Providing Infrastructure as a Service (IaaS) using Prime Service Catalog

Cisco Prime Service Catalog integrated with UCS Director provides single self-service ITaaS catalog for the self-service provisioning and lifecycle management of VMs in the private and hybrid cloud workloads. You can provide services such as provisioning virtual machines on a private cloud using UCS Director and perform the lifecycle operations on these public and private VMs. This section covers the infrastructure services such as virtual machines, fenced containers, Virtual Application Container Services (VACS), and APIC Container Catalog on UCS Director.

Note
- VACS containers are verified and certified only on UCS Director 5.2 platform.
- The public cloud operations are verified and certified on Amazon Web Services (AWS).

Prime Service Catalog also supports Advanced Catalogs from UCS Director. These advanced catalogs are a wrapper around workflows defined in the UCS Director. Prime Service Catalog creates services for these advance catalogs during the UCS Director discovery process. Out of box, these Advanced Catalog-based services can only create requests or objects in UCS Director and do not have any service item dictionary associated with them. However, these generated services can be customized to manage life cycle of objects created through Advanced Catalogs. These services can be customized by adding a service item dictionary, and populating the dictionary with conditional rules. Then, lifecycle operations for the service item can be added via associated services for the service item.

Note Prime Service Catalog currently does not support the popup table input type for UCS Director advance catalog workflow.

Using Prime Service Catalog for Cloud IaaS, you can:

- Create orderable services for VMs and infrastructure containers in hybrid cloud using a unified web interface after integrating with UCS Director. For more information, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.
- Create orderable services for VACS bound VMs and containers.
- Create orderable services for UCS Director based advance catalogs.
- Provide multi-tenant IaaS based on ACI using UCS Director. For more information, see Providing Multi-Tenant IaaS.

Configuring Email Notification on VDC Creation

You receive an email notification when you create a VDC or a standard virtual machine. A VDC can be an APIC, fenced, or VACS container, and a virtual machine can be a standard virtual machine or a cloned virtual machine. You also get an email notification while adding a virtual machine to a Fenced and VACS container.

When you order a new VDC successfully, an email notification is sent out, which includes VDC service item details, VDC subscription data, and specific details of the VDCs such as name, display name, description, cloud name, and status of the VDC with its corresponding virtual machines. You can view the details of all the virtual machines of a particular VDC.

For information on VDC creation, see the "Virtual Data Centers" section in the Cisco Prime Service 11.1.1 User Guide.

For the email notification to work, the following settings must be done:

1   Set the SMTP properties in the **Administration** module. These properties are, "Mail Server Address", "Mail Server Port", and "Support Email Address".

2   FTL files must adhere to the following guidelines:

- FTL files are well formed. This includes naming the tags properly, ensuring that every opening tag has a closing tag, ensuring that at least one "to" address exists, in addition to the other precautions mentioned above.

- FTL files must be placed in some custom template folder and the fully qualified path name to the folder must be specified in **Administration > Settings > Path of the folder containing the FTL files**. The path should navigate to the folder containing the FTL files and not the files itself. By default, these FTL files are available in the "RequestCenter.war/WEB-INF/classes/config/templates/ folder.

- The FTL file path must be in Linux convention (which is a/b/c/d and not a\b\c\d) andmust mandatorily end with '/'.

- For clustered environments, the URL *ObjectCache.Application.URL* must be hardcoded in the *Newscale.properties* file.

- For clustered environments, each node must have the FTL files in the same folder, and this folder must exist in every node.

- FTL files naming convention must not be changed. The FTL files should remain as follows:

    - create_vdc_fen.ftl—For creating Fenced Container VDC

    - create_vdc_apic.ftl—For creating APIC Container VDC

    - create_vdc_vacs.ftl—For creating VACS Container VDC

    - add_vm_fen.ftl—For adding a VM of a Fenced container

    - add_vm_vacs.ftl—For adding a VM to a VACS container

    - vm_operation.ftl—For cloning a VM of a Fenced container and an APIC container, and creating a Standard VM.

3   You can view, modify, show, hide, or remove the FTL file according to your requirement, but do not change the naming convention of the FTL files, as mentioned above. You can view all the details that are included in the email notification.

You can add more than one email address in the **To** field separated by a comma. This field can also contain namespaces, the supported namespaces are: #Requisition.Customer.Email#, #Requisition.Submitter.Email#, #Requisition.Customer.Supervisor.Email#. The To field can also contain a combination of email address and namespace separated by comma. The **From** field is optional. If used, this field can contain only one email address and must not be empty. By default, it is Support Email Address mentioned in the **Administration > Settings** tab. The **Subject** field of the email template can also be customized with a custom subject line for the email.

Note   By default, the <from> field has ToBeFilled as the value. If you want to use the <from> field, edit this field with an appropriate and valid email address. If you do not want to use the <from> field, remove this field or comment it out in the FTL. If the FTL is used as is as provided out of the box, then it would result in an error, since ToBeFilled is not a valid email address.

Apart from the customizations mentioned above, you can also add any static text inside of the FTL template. For this, no special tags need to be used. You can just mention the static text as is. The "subject" field of the email template can also be customized with a custom subject line for the email.

Generating Orderable Services for UCS Director Entities

For creating orderable services for provisioning VMs in cloud, you must perform the following steps:

	Steps	**Topics**
Step 1	Integrate UCS Director with Prime Service Catalog.	Integrating UCS Director (UCSD) or VACS with Prime Service Catalog, on page 118
Step 2	Discover the IaaS entities from UCS Director.	
Step 3	Set up automatic or manual synchronization with UCS Director.	Managing UCS Director Synchronization
Step 4	• Configure search facets, permissions, and presentation for hybrid cloud provisioning services in Prime Service Catalog. • Set up the display category for these cloud services.	• Configuring Permissions and Presentation for Private and Hybrid Cloud Services • Configuring Display Categories for Private Cloud Services

Based on the permissions, end users can now order the hybrid cloud services and perform lifecycle operations on the provisioned containers and virtual machines. For more information on ordering these services, and on the available lifecycle operations for the UCS Director entities, see Cisco Prime Service Catalog 12.0 User Guide.

Integrating UCS Director (UCSD) or VACS with Prime Service Catalog

Using Prime Service Catalog, you can provide infrastructure resources as services and application stack as a service by integrating with Cisco UCS Director (UCSD) and Cisco Virtual Application Container Services (VACS) application. You can manage VMs in hybrid cloud using a unified web interface in Prime Service Catalog after integrating with UCS Director. After integrating with UCS Director and VACS, the types of infrastructure services available in Prime Service Catalog are:

- Container templates, container catalogs, standard catalogs, and advance catalogs from UCS Director

- Container catalog services and container template services from VACS. VACS template services includes a CSR Virtual Machine, VSG Virtual Machine, and application Virtual Machines.

Prerequisites

- To establish an SSL connection, you must add an SSL certificate to the UCS Director or VACS. You can use:

  ◦ A self-signed certificate that matches the hostname or IP address of the UCS Director or VACS server.

  ◦ (Recommended) An SSL certificate that matches the Fully Qualified Domain Name (FQDN) of the UCS Director server signed by a trusted certificate authority.

- If LDAP is integrated, Prime Service Catalog and UCS Director must be integrated with the same LDAP to support single sign-on.

- If you are planning to connect to a UCS Director instance that is integrated with an LDAP, do the following in Prime Service Catalog :

  1 Go to **Administration module > Directories tab > Mappings**.
  2 Map the **Login ID** and **Person Identification** attributes to userPrincipalName.

  Failing to map the above attributes may result in duplicate user accounts in Prime Service Catalog after the UCS Director import.

- Make sure the UCS Director is configured in English.

Step 1 Login to Prime Service Catalog as the Service Admin user.

Step 2 From the main menu, choose **Advanced Configuration > Integrations** and click **New Integrations**.
Note To integrate Prime Service Catalog with VACS, follow the same procedure, which is used to integrate Prime Service Catalog with the UCS Director. However, in this case, you will need to provide the VACS connection details in the **UCS Director** tab.

Step 3 Select **Cisco UCS Director**.
The client/server side validation happens, on successful creation it navigates to Manage Integrations page.

Step 4 Enter the details to connect to the server where UCS Director is installed.
For https connections, import the root CA certificate of the UCS Director server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You can skip the certificate validation by selecting the **Skip Certificate Validation** option.

Step 5 Check **Sync User with IaaS** option to sync this user with IaaS.

Step 6 Check **Enable Poller** if you want to configure automatic polling for the subsequent connections with UCS Director connections.
Note This option is disabled for UCS Director connection that is in Managed Service Provider mode. Manual synchronization is recommended in the UCS Director Managed Service Provider mode.

Step 7 Click **Create Integration**.

Step 8 Select the connection from the Integrations page to and choose **Test Connectivity** option from **Manage Integration** drop-down to authenticate the credentials.

Step 9 After the connection is successful, click **Import all Objects** option from **Manage Integration** drop-down. . The system starts to discover the data from UCS Director. For more information on data discovered from UCS Director, see Cisco Prime Service Catalog 12.0 Designer Guide.
You can now set the timeout period for UCS Director synchronization initiated using the Connect and Import option. Set the ucsddata.killSession parameter in the newscale.properties file to set the timeout. The UCS Director synchronization will end after this set period is elapsed.
Note The UCSD scheduler in the Prime Service Catalog automatically polls UCS Director entities. You can also manually discover these entities using the web interface in Prime Service Catalog. For more information on discovering UCS Director entities in Prime Service Catalog, see Managing UCS Director Synchronization.
Note Once the user is imported to Prime Service Catalog from UCS Director, to login to Prime Service Catalog, the password used must be same as the username.

Step 10 On the **Discovered Panel**, you can:

- View all the discovered entities in the **Objects** tab.

- View the services created for the imported catalog and container entities in the **Services** tab.

    Note   Use the **Overwrite Workflow Form Definition** field in the **Discovered Services** > **Advance Catalog Services** > **General** tab to update advance catalog service form on the Prime Service Catalog side.

- Select a service and configure the category, presentation, facets, and permissions for these services. For more information, see Configuring Permissions and Presentation for Private and Hybrid Cloud Services.

    Note
- Be sure to re-run import, if you add any additional Templates on UCS Director. For example, the Gateway and the Application Server Templates.

- Check the Organization Designer on Prime Service Catalog to see whether the **Service End User** from UCS Director is discovered and is present in Prime Service Catalog.

Deleting a UCS Director connection

As a Service Admin, you can delete a UCS Director connection by selecting the **Remove** option either from Integrations > Setting drop down or Manage Integrations page > Manage Integrations drop down. This option will delete the connection along with its imported entities such as virtual machines, VDCs, containers, templates, catalogs, and workflows.

    Note
- If a UCS Director connection is in the MSP mode, all the associated workflows for that UCS Director instance will also get deleted.

- The templates and catalogs are deleted only when there is no requisition associated with these services.

However, entities such as users, user groups, images, template definitions, and organization units will remain in Prime Service Catalog.

Enabling Single Sign-On in Prime Service Catalog

If you are using Prime Service Catalog in the Cisco ONE Enterprise Cloud Suite, you must enable single Sign-on (SSO) when integrating Prime Service Catalog with UCS Director.

    ⚠️

Caution   You cannot configure both LDAP and SAML configured for SSO login in Prime Service Catalog. If you wish to use LDAP SSO, the SAML SSO must be manually disabled, failing which will lead to incorrect login behavior. To disable SAML login, go to **Administration > Settings > Customizations**. From the Common section, turn off the **Enable SAML setting** and click **Update**.

Prime Service Catalog and UCS Director use LDAP authentication to handle permissions for catalog items and service items. With LDAP integration, group permissions for the catalog items and virtual machines in UCS Director are synchronized with the service items and catalog items in Prime Service Catalog. For example, if a specific group owns a virtual machine in UCS Director, the users in that group can view the same virtual machine in Prime Service Catalog. In addition, if a specific group can access a catalog item in UCS Director, the users in that group can order the same catalog item from Prime Service Catalog.

Use the procedure below to enable the single sign-on:

Step 1 Set up LDAP integration in Prime Service Catalog. For more information, see the *Configuring LDAP integration* section in Cisco Prime Service Catalog 12.0 Integration Guide.

Step 2 Set up LDAP integration in UCS Director. For more information, see the *LDAP Integration* section in Cisco UCS Director 5.3 Administration Guide.

    Note Ensure that the LDAP groups that you are using are imported from Prime Service Catalog to UCS Director. After importing to UCS Director, ensure that you manually synchronize the users and user groups in UCS Director.

Step 3 Integrate UCS Director with Prime Service Catalog. For instructions on integrating UCS Director with Prime Service Catalog, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog, on page 118.

    Note In Prime Service Catalog, ensure that you check the **Export User** check box in the **Manage Connections** tab, so that only the users and groups with LDAP authentication are exported from UCS Director.

Managing UCS Director Synchronization

- Scheduling UCS Director Synchronization
- Manually Importing UCS Director Synchronization
- Scheduling the Collection of Reporting Data from UCS Director

Scheduling UCS Director Synchronization

You can automatically discover UCS Director instances at scheduled intervals using the scheduler. Use the below procedure to configure the scheduler.

Step 1 Edit the following properties files. These files can be located in the **RequestCenter.war/WEB-INF/classes/config** directory.

- In the **newscale.properties** file, change the interval of polling, as shown in the example below:

```
###########################################
#Data Poller
###########################################
#Cron Expression wakes up poller every 10 minutes of an hour
ucsddata.poller.cron=0 0/10 * * * ?
#Cron Expression wakes up health check for 3rd min and 5 mins thereafter of the hour ex: 03,08,13
 minutes
uscddata.poller.health.check.cron=0 3/5 * * * ?
#High Availability Health checks threshold, this should be greater than Poller cron time specified
 in minutes
ucsddata.healthCheck.threshold=15
# Number of minutes after which button to kill poller shows up on the manage connections UI
uscddata.killSession=30
```

• In the **support.properties** file, set the poller value as "true", as shown below:

```
###### Data Poller Settings ###################
# In non-cluster mode: this should be enabled for the Requisitions Data script to be run from
the Poller
# In clustered mode: this can be either enabled on all nodes in the cluster OR on a specific
node in the cluster
# - only 1 node in the cluster will run at any given time, even if this is enabled on multiple
 nodes in a cluster (which ever node starts it first)
ucsdData.poller.enable=true
###########################################
```

Step 2   In **Administration** > **Settings** page, select the **UCSD Scheduler** option.

Note   • The following step is critical for automatic synchronization.

• All entities except Users will be automatically synchronized if you have enabled the Scheduler. Any change in User on UCS Director should be manually synchronized in Prime Service Catalog. For more information on manual synchronization, see .

Manually Importing UCS Director Synchronization

If Prime Service Catalog and UCS Director are integrated with LDAP, it is recommended to manually poll users information using the web interface whenever the user roles are changed in UCS Director. This is to ensure synchronization of the user's RBAC permission to Prime Service Catalog services with the changes made in UCS Director.

You can manually import UCS Director instances using the UCS Director Integration page. When you perform this process, all entities including users and roles are synchronized.

This process is used in the following scenarios:

• If you do not want to use a Scheduler.

• If you are using a Scheduler and UCS Director and Prime Service Catalog are integrated with LDAP. To improve the performance, the Scheduler does not synchronize users and roles. Because of this behavior, if an administrator makes changes to users and roles in UCS Director, these changes are not communicated to Prime Service Catalog. To synchronize these changes with Prime Service Catalog, you must manually import UCS Director instances, which in turn synchronizes the users and roles.

Step 1   Choose **Advanced Configuration > Integrations** (Integrations) page.

Step 2   Select the UCSD instance and select **Manage Integration** option from **Settings** drop down.

Step 3   Click **Import All Objects** option from **Manage Integration** drop-down.

Scheduling the Collection of Reporting Data from UCS Director

You can discover the reporting data for all VMs from the UCS Director at scheduled intervals, using the scheduler, automatically. You can also configure the number of days, months, weeks and beginner of the week for which the data needs to be imported and displayed in the Prime Service Catalog. Use the following procedure to configure the scheduler and the reporting data settings.

Edit the following properties files. These files are located in the **RequestCenter.war/WEB-INF/classes/config** directory.

- In the **newscale.properties** file, change the interval of polling, as shown in the example below:

```
############################################
#Resource Reporting Data Poller
############################################
#Cron Expression wakes up poller every 43 minutes of an hour
• reportsdata.poller.cron=0 10/20 * * * ?
#Cron Expression wakes up health check for 13th min and 15th min thereafter of the hour ex:
13,28,43,58 minutes
reportsdata.poller.health.check.cron=0 17/20 * * * ?
#High Availability Health checks threshold, this should be greater than Poller cron time specified
 in minutes
reportsdata.healthCheck.threshold=127
```

- In the **newscale.properties** file, add the number of months, days, weeks, and set the beginner of week, as shown in the example below:

```
############################################
#Resource Reporting Import Data Settings
############################################
#This property is configurable setting to fetch monthly usage data for first import.
#This is max value. If any value more than 12 is overwritten with 12.
• reportsdata.import.numberofmonths=12
#This property is configurable setting to fetch daily usage data for first import.
#This is max value. If any value more than 365 is overwritten with 365.
• reportsdata.import.numberofdays=365
#This property is configurable setting to fetch weekly usage data for first import.
#This is max value. If any value more than 52 is overwritten with 52.
• reportsdata.import.numberofweeks=52
#This property is configurable setting to fetch weekly usage data for first import.
#Only Monoday or Sunday or the values for this property. Otherwise Monday will be picked
#for any other day provided here.
• reportsdata.import.beginnerofweek=Monday
```

- In the **support.properties** file, set the poller value as "true", as shown below:

```
###### Reporting Data Poller Settings ##################
# In non-cluster mode: this should be enabled for the Requisitions Data script to be run from
the Poller
# In clustered mode: this can be either enabled on all nodes in the cluster OR on a specific
node in the cluster
# - only 1 node in the cluster will run at any given time, even if this is enabled on multiple
 nodes in a cluster (which ever node starts it first)
reportsData.poller.enable=true
############################################
```

Configuring Permissions and Presentation for Private and Hybrid Cloud Services

Based on the permissions granted to an end user, the discovered services from UCS Director becomes orderable in the **Service Catalog** module.

To understand the UCS Director groups and roles mapping to Prime Service Catalog groups and roles, see Prime Service Catalog System Defined Roles for UCS Director Integration and Users and User Groups Imported from UCS Director.

Depending on the UCS Director integration, you can discover standard catalogs, container catalogs, and container templates services for end-user provisioning and maintenance of VMs on private and public cloud. Using these services, end users can:

Order services created based on service container catalog, standard catalog, advanced catalog, and fenced container templates from UCS Director.

Before You Begin

Discover the Services from UCS Director by integrating with the UCS Director instance. For more information on integrating UCS Director, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 1   Select the connection from the Integrations page and select **Manage Integration** option from **Settings** drop down.

Step 2   Click **Services** button in **Discovered** panel.

Step 3   Double-click on the service to be customized.

Step 4   In the **Details** panel, enter Service Name, Description, and add Categories.

> **Note**   Private Cloud Iaas will be selected as the default service category for UCS Director services. You can remove the default category and associate the generated services to another category. A service can also be associated with multiple categories.

> **Note**   New Categories can also be created and one category image can also be associated with that newly created category and this new category can be associated with existing service.

For an advance catalog services, select **Yes** in the **Overwrite Form Definition** field, if you want to overwrite Custom Form Rules, Display Properties, and Dictionary Names for these services. And click **Save**.

Step 5   In the **Presentation** panel, click **Attach**, to select an image to be associated with the service or select **Image URL** to enter the URL of the image. Default option selected is **Image File**.

Step 6   Select an image from the list of **Select Image** window and click **Add**.

Cisco provides a number of images out-of-box that you can assign to the service. You can also upload an image to be used for the service.

Step 7   Enter a description for the service by selecting the **Overview** or **Service Form** options, and click **Save**.

Step 8   In the **Facets** panel, choose the required options and click **Save**.

Step 9   In the **Permissions** panel, do the following:

- Select the roles from the list and click **Remove Selected** to remove the permission.

- Select from the **Add Permissions** drop-down list to add or select the roles from the list who can deploy these services.

- **For container templates, container catalogs, standard catalogs, and advance catalogs services created in Prime Service Catalog for UCS Director**:

  ◦ If these services are associated to a group in UCS Director, users in the corresponding group in Prime Service Catalogs can only order services that the group has access to.

  ◦ If the services are associated to All Groups in UCS Director, users in the corresponding group in Prime Service Catalog can order the services that All Groups have access to.

Step 10   Click **Save**.
The new service will be displayed in the **Service Catalog** module based on the category you have selected.

Mapping Templates for UCSD Services

Prime Service Catalog provides out-of-box templates using which you can map to the UCSD services. The template service defines the way the entities of UCSD appear as a service in Service Catalog module. In UCSD, templates can be mapped at catalogs or templates level.

Custom templates can be created based on the out-of-box UCSD templates provided by Prime Service Catalog and used for mapping to the UCSD services. For more information on creating custom templates see, *Create Custom Templates* in Cisco Prime Service Catalog Designer Guide.

To map a template:

Step 1   Select the connection from the Integrations page, choose **Manage Connection** from the settings.

Step 2   Click **Objects** in the **Discovered** panel.

Step 3   Choose the *Template* or *Catalog* from the left hand side and for the selected entry, choose the custom template from the **Select Base Template** drop-down list.

Step 4   You can do one of the following from the settings option:

a) Click **Regenerate Service**, to regenerate the existing service with the selected new template.

b) Click **Generate Service Variant**, to create a service variant corresponding to the UCSD entities with the new custom template.
    Note   If this service variant already exists for the selected template, then it will be regenerated.

Users and User Groups Imported from UCS Director

Note In a single pane of glass, where Prime Service Catalog, UCS Director are connected to LDAP:

- The Home OU of a user is always determined by LDAP mapping .

- The User gets group membership of UCS Director if the user belongs to UCS Director imported groups.

- If the User data that is imported (discovered) does not exist in Prime Service Catalog, the same is created in Prime Service Catalog and the normal flow for OU, Group and Role is executed.

When Prime Service Catalog connects to a UCS Director for the first time, Prime Service Catalog creates a:

- **UCSD ::<ID>::All Groups:**

Where <ID> is the 3-letter identifier of the UCS Director server. This group will be the parent group for all groups imported from this UCS Director server.

- **UCSD ::<ID>::<Group Name>**:

Where <ID> is the 3-letter identifier of the UCS Director server. There will be group for each group in the UCS Director. All such groups are grouped under the parent group. Users belonging to various groups in the UCS Director are imported to the respective groups in Prime Service Catalog.

- **Default group**. The default group is grouped under the parent group. Users without a group in the UCS Director are imported to this group.

All the imported users from the UCS Director are assigned an Organizational Unit (OU) in Prime Service Catalog.

During the subsequent connections, Prime Service Catalog checks for group membership changes and updates the records accordingly.

Note For container templates, container catalogs, standard catalogs, and advance catalogs services created in Prime Service Catalog for UCS Director:

- If these services are associated to a group in UCS Director, users in the corresponding group in Prime Service Catalogs can only order services that the group has access to.

- If the services are associated to All Groups in UCS Director, users in the corresponding group in Prime Service Catalog can order the services that All Groups have access to.

Prime Service Catalog System Defined Roles for UCS Director Integration

Prime Service Catalog creates the following system-defined roles for the UCS Director roles it discovers. The following table lists the mapping of the UCS Director to Prime Service Catalog system-defined roles.

Table 45: Prime Service Catalog Roles Mapping with UCS Director Roles

UCS Director Roles	Prime Service Catalog System Defined Roles	Description
System Admin All Policy Admin Computing Admin	UCSD Sys Admin	UCSD Sys Admin user can view the details of Containers, vDC's and VM's as service items in My Products and Services based on the Group permissions assigned to each of the UCS Director Service Item in Service Item Manager. Only users with this role can order Container Template Services.
Service End-User, Group Admin, Operation roles	UCSD End User	UCSD End User can view the details of Containers, vDC's and VM's as service items in My Stuff based on the Group permissions assigned to each of the UCS Director Service Item in Service Item Manager. Users with this role can order services based on the group to which user belongs and catalogs which are assigned to a group in UCS Director.
All other roles	UCSD Operator	Users with this role can only view and use the self-service portal but cannot order the services.

Note In a single pane of glass, where Prime Service Catalog, UCS Director are connected to LDAP:

- The Home OU of a user is always determined by LDAP mapping .

- The User gets group membership of UCS Director if the user belongs to UCS Director imported groups.

- If the User data that is imported (discovered) does not exist in Prime Service Catalog, the same is created in Prime Service Catalog and the normal flow for OU, Group and Role is executed.

Configuring Display Categories for Private Cloud Services

The new service will be displayed in the **Service Catalog** module based on the category you have selected.

Before You Begin

Discover the Services from UCS Director by integrating with the UCS Director instance. For more information, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 1   Choose **Advanced Configuration > Integrations** and select the connection from the Integrations page.

Step 2   Click **Manage Integration** option from drop down and click on the **Services** tab in the Discovered panel double-click on the service.

Step 3   In the **Details** panel, do the following:

    a) Enter a service name and description for the selected service.

    b) Select an existing category or create a new category by clicking on the **New** option.

Step 4   Click **Save**.

Providing Multi-Tenant IaaS

This feature enables service providers to use **Cisco ONE Enterprise Cloud Suite** to provide multi-tenant Infrastructure as a Service (IaaS) on ACI. The components required for this functionality are: Prime Service Catalog, UCS Director (in **Managed Service Provider** mode), and ACI.

The **Tenant Management** module in Prime Service Catalog provides infrastructure services to multiple tenants quickly and efficiently. Using this module, tenants can manage their own set of services, and offer these infrastructure services to their end users. A tenant can contain several organizations and each organization can contain several users.

Using **Tenant Management** module:

- A tenant administrator can manage tenant users, define quotas on computing resources and virtual machines for a tenant user, and delegate management of firewalls and load balancers.

- An end user can self-service provision and manage VMs.

The tenant workflow (for example: create, update, and delete tenants), VDC, and VM operations are executed through Advanced and Service Container Catalog workflow in UCS Director. Prime Service Catalog creates services for these advance and service container catalog workflows during the UCS Director discovery process. For this feature to work seamlessly, a site administrator must map these UCS Director discovered services to the Tenant Management workflow in Prime Service Catalog. For more information, see Setting Up Tenant Management Module and Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director .

Tenant Workflow Configurations in UCS Director for Multi-Tenant IaaS

For seamless multi-tenant IaaS operations, an administrator must ensure that multi-tenant IaaS-related objects are created and configured in UCS Director. An administrator need to configure only four of these multi-tenant IaaS workflows. Remaining workflow are pre-defined and configured during the installation process.

This section covers the list of fields or attributes that must be configured for these workflows in the UCS Director. For more information on how to create these advance and container catalog workflow, see Cisco UCS Director 6.0 Administration Guide.

Note Do not use hyphen in UCS Director Advance Catalog name. This is to avoid the synchronization issues after integrating with Prime Service Catalog.

Table 46: Configurations for Multi-Tenant IaaS Workflows on UCS Director

UCS Director Workflow	UCS Director Advance or Service Container Catalog Fields
VNX Tenant Onboarding	• **CPU Reservation (MHz) - (Sample Value - 10000):** Value for this attribute must be derived by an Analyst or an Administrator. • **Capacity (EMCSizeUnit) (Sample Value - GB)** • **Tenant Profile** : Application caters to only one profile. • **Service offering** : Application caters to only one offering. • **Service Profile** : It is a mandatory value. Map this to an existing profile in the system. • **Physical Server Reserved Space** • **Datastore Size Limit (GB)** • **VM Over Subscription** • **L2 VLan ID** • **L2 IP Subnet**
Update Tenant	• **Tenant Profile Name:** Application caters to only one profile. This field should be same as specified in VNX Tenant Onboarding workflow. • **Service Offering:** Application caters to only one service offering. This field should be same as specified in VNX Tenant Onboarding workflow • **CPU Reservation (MHz):** Value for this attribute must be derived by an Analyst or an Administrator. • **Service Profile Identity:** It is a mandatory value. Map this to an existing profile in the system. • **Capacity (GB)** • **Datastore Limit**
APIC Service Container catalog	No specific fields to configure for APIC Service Container catalog. Make sure an APIC Service Container catalog is available in UCS Director for VDC workflows.

UCS Director Workflow	UCS Director Advance or Service Container Catalog Fields
Firewall Rule Action Configuration	• **Firewall ID** • **Protocol** • **Entry Name** • **Order** • **Service Param** • **Source Address** • **Source Any** • **Source Port** • **Tag**

Setting Up Tenant Management Module

A site administrator must perform the following steps for seamless multi-tenant IaaS operations.

Before You Begin

- Connect to a UCS Director instance that is in the Service Provider mode.

- In Prime Service Catalog, **Service Link** module, verify that **UCSD Agent** is up and running.

- Verify that tenant management-related objects are created and configured in UCS Director. For information on the advance and container catalog workflow inputs that are configured on the UCS Director, see Tenant Workflow Configurations in UCS Director for Multi-Tenant IaaS.

Step 1   Integrate Prime Service Catalog with UCS Director and discover the infrastructure entities from UCS Director. For instructions, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 2   Map the Advanced Catalog/Container Catalog services from UCS Director to the Prime Service Catalog workflow. For more information, see Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director .

Step 3   Invoke workflow for creating tenants in Prime Service Catalog. For more information, see Onboarding a Tenant.

Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director

When Prime Service Catalog is integrated with UCS Director, the discovery process creates services based on UCS Director Advanced Catalogs and APIC service container catalog. The advance and the APIC service container catalogs in UCS Director are used for publishing workflow for creating, managing a tenant and creating a VDC respectively.

For a seamless multi-tenant IaaS operations, a site administrator must map these services with the UCS Director workflows.

Note Only four of the Prime Service Catalog tenant management workflows need mapping from an administrator. The remaining workflows are pre-defined and are configured during the installation process. For information on the workflows that needs mapping in Prime Service Catalog, see the table below .

Before You Begin

Integrate Prime Service Catalog with UCS Director instance that is in the Service Provider mode. For more information, see Integrating UCS Director (UCSD) or VACS with Prime Service Catalog.

Step 1 Discover the UCS Director entities in Prime Service Catalog.

Step 2 On the discovery page in Prime Service Catalog, select a workflow from the **Manage Workflows** section and click to open manage workflow page. , and select an advance or a service container catalog service from the **Services** drop down on the right-hand side. For information on which services to select in this drop down, see the table below.

Step 3 Based on the type of advance or service container catalog service selected in the previous step, select the values for the remaining workflow attributes and click **Save**.

Note
- Most of the attribute mappings are self explanatory except Organizational Unit. Organizational Unit should be mapped to GroupName.

- You can introduce custom attributes in the PSC service to map any new workflows in UCSD Advance or Service Container Catalogs using the **Add Attribute** option. If the new catalogs are not mapped to the PSC service, requisition is not created and an error is displayed. The custom attributes can be modified or deleted if the catalogs are not in use.

Step 4 Navigate to **Tenant Management** module and invoke workflow for creating tenants. For VDC and Firewall Rule Workflows, navigate to **Service Catalog** module **My Products & Services** > **Virtual Data Centers** to create VDC and add Firewall Rule.

The status of the service request is displayed as Completed, if the operation on UCS Director is successful.

Note If the attributes are not mapped properly, requisition is not created and an error is displayed.

Prime Service Catalog Workflow	UCSD Advance/Service Container Catalogs
Create Tenant	Advance Catalog based on **VNX Tenant Onboarding** workflow
Manage Tenant	Advance Catalog based on **Update Tenant** workflow
Create VDC	Advance Catalog based on any **APIC Service Container Catalog**
Create Firewall	Advance Catalog based on **Firewall Rule Action Configuration** workflow

Onboarding a Tenant

As a site administrator, you can create a tenant administrator. A Tenant administrator can create and manage users, Organization Units (OUs), and VDCs. In addition, the tenant administrator can specify which tasks the users can perform on their virtual machines and services, and can place quotas on computing resources and virtual machines.

When you create a Tenant Admin, the Organization and Tenant User dashlets are automatically created and associated for that Tenant.

The following prerequisites must be met before the site administrator creates a tenant:

Note   These prerequisites are also applicable for creating a VDC.

Before You Begin

- Add a UCS Director connection that is in the Manage Service Provider (MSP) mode. You can connect to a UCS Director instance in **Advanced Configuration** > **Integrations** and click **New Integrations**.

- Map the advance/service container catalog services with the Prime Service Catalog workflows. For more information, see Mapping Tenant, VDC, and Firewall Rule Workflows from UCS Director .

- UCSD Agent must be up and running in the Service Link module.

Step 1   Log in as Site Administrator.

Step 2   Go to **Tenant Management**.

Step 3   Click **Add Tenant** from the **Tenant Management Dashboard**.

Step 4   In the **Tenant Information** tab, enter details such as name of the tenant, address, disaster recovery protection information, L2 VLAN ID, L2 IP Subnet, Tenant IP Pool, and Resource Selection (For ND).

Note   • L2 VLAN ID, L2 IP Subnet, and Tenant IP Pool attributes are required to map the appropriate subnet inside a container. Enter the L2 VLAN ID, L2 IP Subnet, and Tenant IP Pool in the recommended format as shown on the web interface.

- Editing tenant details after the tenant is created will cause the L2 VLAN ID, L2 IP Subnet, and Tenant IP Pool fields to be in a read only state.

- If you choose the Provision New Resources option from the Resource Selection (For ND) drop-down list, you must enter the details for RAM (For ND), vCPU (For ND), and Storage (For ND).

Step 5   Specify the reservation details for vDC in the **Quota Management** tab (based on the vDC template).
UCS Director uses this information for resource allocation and to provision that tenant. The Tenant Administrator can then create and manage OUs, vDC, and users for each of the associated Tenant.

When the Tenant is in the **Being provisioned** status, the Tenant Admin icon will be disabled on Tenant Dashboard restricting the user (site admin) to view the User Management. An information icon 'i' is displayed in Status in the Tenant Dashboard and when clicked, displays an overlay of requisition, provisioning workflow summary, comments with date and timestamp.

You can also search and edit only the quota/capacity details (and not any other details associated to a VDC) by navigating to **Tenant Management** > **Find a Tenant**. The Tenant Administrator can navigate to Organization, Users, and VDCs from the User Dashboard.

Note
- The Tenant Admin icon (next to Status column) is enabled or disabled based on the Status of the Tenant. If the Tenant is Active, you can navigate to User Management by clicking the Tenant Admin icon to perform necessary tasks.

Deleting a Tenant

The following instructions are specific only to the customers who have access to the Tenant Management module.

To delete a tenant from the **Tenant Management** dashboard, make sure that you delete all the physical servers, VMs, VDCs, Organization users, or any service items associated with that tenant. Follow the steps in the same sequence as listed below.

There might be slight variations in steps depending on the database you are using.

Step 1 (As a Tenant Administrator) Go to **Service Item Manager > Manage Service Items**, then click the delete icon to delete physical servers for the tenant.

Step 2 Go to **My Products & Services > Virtual Data Center**, then select the VDCs corresponding to the tenant.

Step 3 Delete the load balancer. To delete, select the Load Balancer from the **Load Balancer** tab and click the delete icon.

Step 4 Delete the Firewall rule. To delete, select the **Firewall rule** from the **Firewall Rule** tab and click the delete icon.

Step 5 Delete the VMs. To delete, click the **Virtual Machines** corresponding to the VDC. On the right of each VM, click the gear icon to delete it.

Step 6 Delete the VDCs. Click the delete icon on the existing VDC to delete it.

Step 7 (For Oracle only) Go to the **Administration > Utilities** and purge all the requisitions for the specific users.

Step 8 Go to the **Organisation Designer** module and do the following:

    1 Move all the OUs to some other parent OU, which is not a tenant.
    2 Remove the additional OUs (Other than Home OU) for users and then delete users.
    3 Delete the users by clicking the **Remove** button.

Step 9 (As a Site Administrator) Go to the **Tenant Management** module and click the delete icon next to the tenant, which you want to delete.

Providing CloudCenter Applications as a Service

Cisco Prime Service Catalog offers a direct integration with Cisco CloudCenter. You can set up the connection from Prime Service Catalog to CloudCenter, resulting in the automated import of the application deployment workflows, ready to be published to the catalog.

CloudCenter lets users define cloud-agnostic blueprints of their multi-tier applications and then deploy them to private, public, or hybrid clouds based on cost and performance metrics provided by CloudCenter. CloudCenter can manage the lifecycle of an application with auto-aging policy and the ability to scale-out and scale-in individual tiers of a multi-tier app based on application performance.

Generating Orderable Services for CloudCenter Applications

For creating orderable services for deploying CloudCenter applications in cloud, you must perform the following steps:

	Steps	Topics
Step 1	Integrate CloudCenter with Prime Service Catalog.	Integrating CloudCenter with Prime Service Catalog, on page 134
Step 2	Discover application profiles.	
Step 3	Configure search facets, permissions, and presentation for hybrid cloud provisioning services in Prime Service Catalog.	Configuring Permissions and Presentation for CloudCenter Services, on page 136

Based on the permissions, end users can now deploy the application services.

Integrating CloudCenter with Prime Service Catalog

As a Service Administrator you can add a connection to CloudCenter server, and imports Application Profiles and Activation Profiles from CloudCenter database. For each CloudCenter application profile, Prime Service Catalog automatically creates a service.

Prerequisites

- Configure SAML to integrate Prime Service Catalog and CloudCenter to support single sign-on.

- To integrate CloudCenter with Prime Service Catalog follow the below procedure:

Step 1 Login to Prime Service Catalog as the Service Administrator (or Site Administrator) user.

Step 2 From the main menu, choose **Advanced Configuration** > **Integrations** and click **New Integrations**.

Step 3 Select **Cisco CloudCenter**.

Step 4 Enter the details and click **Create Integration** to connect to the CloudCenter server.

1 For https connections, import the root CA certificate of the CloudCenter server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You could Skip the certificate validation by selecting the **Skip Certificate Validation** option .

2 API is a mandatory field, you must obtain the username and API key from CloudCenter to connect to the CloudCenter server.

3   By default, a base template is mapped to the connection. However, you can use other templates available in the drop-down list. For more information on Service Templates see section Mapping Application Templates for CloudCenter, on page 136.

Step 5   Choose **Test Connectivity** option from **Manage Integration** drop-down to validate the credentials and the server details.

Step 6   After the connection is successful, click **Import all Objects** option from **Manage Integration** drop-down . The system starts to discover and import the published CloudCenter application profile .

Step 7   In the **Discovered** panel, you can:

- View all the discovered entities in the **Objects** tab.

- View the services created for the Application in the **Services** tab.

- Select a service and configure the category, presentation, facets, and permissions for these services. For more information, see Configuring Permissions and Presentation for CloudCenter Services, on page 136.

Deleting a CloudCenter Connection

You can delete a CloudCenter connection by choosing **Remove** option from **Manage Integration** or by choosing **Remove** option from **Settings** drop down in the Integrations page. This option will delete the connection along with its imported entities such as applications and activation profiles.

Enabling Security Assertion Markup Language (SAML) SSO in Prime Service Catalog

Security Assertion Markup Language (SAML) can be used with Prime Service Catalog to provide external authentication of users and a means of SSO (Single Sign-On).

As a prerequisite to integrate Prime Service Catalog with CloudCenter, you must enable and configure SAML SSO.

Perform the following procedure to enable single sign-on:

Step 1   Enable SAML on Prime Service Catalog:

a) Go to **Administration > Settings > Customizations**.

b) From the Common section, turn on the Enable SAML setting and click **Update**.

Step 2   Configure SAML support in Prime Service Catalog. For more information, see the *Configuring SSO Using SAML* section in Cisco Prime Service Catalog 12.0 Integration Guide.

Step 3   (Optional) Integrate CloudCenter with Prime Service Catalog. For more information, see Integrating CloudCenter with Prime Service Catalog, on page 134.

Configuring Permissions and Presentation for CloudCenter Services

Based on the permissions granted to the user, the discovered application services become available in the **Service Catalog** module. Using the options described in the below procedure you can grant deploying permission of these services to OUs, users, groups or roles in prime Service Catalog, or customize the services by adding more presentation details, descriptions, categories, etc. However, the services are ready to be deployed as is without any additional definitional changes.

Before You Begin

Discover the Application Profiles from CloudCenter by integrating with the CloudCenter. For more information on integrating, see .

Step 1 Select the connection from the Integrations page and click **Services** in the **Discovered** panel or select **Manage Integration** option from **Settings** drop down and click **Services** in the **Discovered** panel.

Step 2 Select the service to be customized.

Step 3 In the **Details** panel, enter Service Name, Description, and add Categories. And click **Save**.
Note CloudCenter Applications will be selected as the default service category for CloudCenter services. You can remove the default category and associate the generated services to another category. A service can also be associated with multiple categories.

Step 4 In the **Presentation** panel, click **Attach**, to select an image to be associated with the service or select **Image URL** to enter the URL of the image. Default option selected is **Image File** .

Step 5 Select an image from the list of **Select Image** window and click **Add** . Cisco provides a number of images out-of-box that you can assign to the service. You can also upload an image to be used for the service.

Step 6 Enter a description for the service by selecting the **Overview** or **Service Form** options, and click **Save** .

Step 7 In the **Facets** panel, choose the required options and click **Save**.

Step 8 In the **Permissions** panel, do the following:

- Select the roles from the list and click **Remove Selected** to remove the permission.

- Select from the **Add Permissions** drop-down list to add or select the roles from the list who can then deploy these services.

Step 9 Click **Save**.
The new service will be displayed in the **Service Catalog** module based on the category you have selected.

Mapping Application Templates for CloudCenter

You can set a base template for the services for a chosen connection or the application profile. This template defines the way the application appears as a service in Service Catalog module.

The templates can be mapped at two levels:

- **Connection level**: You can map the template when you add a new connection or modify the connection later to map a new template. On import all the applications associated with that connection inherit the template assigned at the connection level.

Note Only those template will continue to inherit connection level template which were inheriting before connection level template is changed.

- **Application Profile level**: Templates can also be assigned at application profile level. You can create custom templates in Service Designer based on the out-of-box template for CloudCenter, these custom templates will then be available for mapping to the Application Profiles. For more information, see Cisco Prime Service Catalog Designer Guide.

Note It is recommended to apply the custom templates at application profile level only in the case current template for that application profile is updated and you want the service to have those changes.

To map templates at application profile level follow the below procedure:

Step 1 Select the connection from the Integrations page and click **Objects** in the **Discovered** panel.

Step 2 Choose the Application Profile from the list and select the new template from the **Select Base Template** drop-down list.

Step 3 You can do one of the following from the settings option:

a) Click **Regenerate Service**, to regenerate the existing service with the selected new template.

b) Click **Generate Service Variant**, to create a service variant corresponding to the application profile with the new base template.

   Note If this service variant already exists for the selected template, then it will be regenerated.

User Management in CloudCenter

With SAML support enabled, with the first login of the IDP user a corresponding Prime Service Catalog user is created. When a user joins or creates a Tenant for the first time, this user is pushed in to CloudCenter and is associated to the default Activation Profile.

Integrating Performance Manager with Prime Service Catalog

As a Service Administrator you can add a connection to Performance Manager server. Data points for performance reports are generated in UCS Performance Manager. Prime Service Catalog imports these data points through an API call functionality. For each Performance Manager application profile, Prime Service Catalog automatically creates a service. You can view the performance report for a vDC for an hour, 6 hours, and 1 week. You can also customize the time interval for which you need the performance report. For more

information on performance reports, see section *Viewing Performance reports* in Cisco Prime Service Catalog User Guide.

Before You Begin

Ensure to have UCSD connection established and VMs created by UCSD user in Prime Service Catalog.

Step 1   Login to Prime Service Catalog as the Service Administrator user.

Step 2   From the main menu, choose **Advanced Configuration > Integrations** and click **New Integrations**.

Step 3   Select **Cisco UCS Performance Manager**.

Step 4   Enter the details to connect to the server where UCS Performance Manager is installed.
For https connections, import the root CA certificate of the UCS Performance Manger server. Copy the content of the root CA certificate of the server and paste it in the text area. If the root certificate is a chain of certificates, paste the content one below the other. The connection would fail, in case the SSL certificate of the server becomes invalid or untrusted. You can skip the certificate validation by selecting the **Skip Certificate Validation** option.

Step 5   Click **Create Integration**.

Step 6   Select the connection from the Integrations page to and choose **Test Connectivity** option from **Manage Integration** drop-down to authenticate the credentials.
Note   The UCSPM scheduler in the Prime Service Catalog automatically polls UCS Performance Manager entities.

Deleting a UCS Performance Manager Connection

As a Service Administrator, you can delete a UCS Performance Manager connection by selecting the **Remove** option either from Integrations > Setting drop down or Manage Integrations page > Manage Integrations drop down. This option will delete the connection along with its imported entities such as application and activation profiles, clouds, and deployment environments..

Deploy Team Management

- Deploy Team Management, page 139

Deploy Team Management

Prime Service Catalog provides the ability to support multi-team environments. A multi-team environment enables the division of large organizations into logical entities called teams. As a result, you can achieve logical isolation between teams and manage the permissions to order services to the entire team or project. Team Management is provided as a service pack with Prime Service Catalog. You can choose to activate it to use the team management functionality.

Prime Service Catalog provides a strict organizational hierarchy as follows:

1 Project

2 Team

3 Sub Team

Project is a root team and can have multiple teams. Each team can have multiple sub teams. By default the users go not have permissions to order any services. It's the Site Administrator or Service Administrator's responsibility to grant permission to a Project or Team for a service through Integrations or Service Designer. When the permissions are granted at Project level, all the users who belong to the Project can order the service. However, any permission for services granted at team level are only available for the users that are below it in the same hierarchy.

For example, if a system has sub teams named Team A and Team B, Team A cannot order services granted for the Team B. Team B cannot order any services granted for the Team A. However, both Team A and Team B can order services available for the Project.

On the Prime Service Catalog side, when a Project is created a corresponding account is created. And when a team or sub team is created, a corresponding OU is created. OU is used to leverage permissions to the teams and sub teams. OUs have the same name as the Team/sub team corresponding to them. Permissions on the Service Items created as a result of the deployments or server creations are assigned to the Team OU of the user.

Once team management is activated, every Prime Service Catalog user must belong to a team to be able to order services. When the user first navigates to Teams page from the main menu, the user is provided with

two options. User can join an existing team or create a new team. In this release a user can be a member of only one team regardless of his role.

The below table lists the High-level roles and their respective tasks in Team Management. For more details of the roles and capabilities see, Application Roles and Capabilities, on page 78.

Table 47: High-level roles and Tasks in Team Management:

Role	Tasks
Site Administrator	Deploys/Activates Team Management. Creates Service Administrator Role.
Service Administrator	Creates integrations with UCSD and CloudCenter, discovers entities and objects from UCSD and CloudCenter. Configures search facets, permissions, and presentation of the services. Assigns the Service Admininstrator role to other users using the *Create Service Admin* service.
Team administrator	Approves the permission for a new member to join the team or create a sub team under the current team. Views the assets and deployments for the entire team hierarchy.
User	Joins an existing team or creates a new team (in this case this user becomes a Team Administrator). The User can deploy only those applications and services to which they have permissions to order. This person can perform life cycle operation on deployments or servers he/she owns.

Activating Team Management

Once you have understood how the team management works, as a Day-0 configuration, you must activate Team management module. Only the Site administrator role has capability to activate Team Management. Only when Team Management is activated, the **Teams** menu is available in the main menu for all other users.

Warning   In the 12.0 release, once you enable Team Management, you cannot disable it.

To activate Team Management:

Step 1   Log in as the Site Administrator.

Step 2   From the main menu, choose **Teams**.

Step 3   Click **Activate now** and accept the terms and conditions.
The deploy team management service form appears.

Step 4   Enter the details in the service form and click **Submit**.

Field	Description
Name	Enter a name for the team management configuration.
Billing	Choose whether the billing is active or inactive. If billing is selected as active the following three fields appear for selection.
Billing type	Choose the billing type for the teams from the drop-down list. You are allowed to choose multiple options from the list.
Billing Department	Indicates that the billing department can be a free form text.
Team admin approval required	Specify whether the join team or create team action need approval.
Department	Specify the user's department in the organization.

Create Integration

A service administrator creates integrations with UCSD and CloudCenter and governs the permissions on the services. For more information on integration with UCSD and CloudCenter see, sections Integrating UCS Director (UCSD) or VACS with Prime Service Catalog, on page 118 and Integrating CloudCenter with Prime Service Catalog, on page 134.

The service administrator can assign unique services to each team through the related OUs. For more information see section Configuring Permissions and Presentation for CloudCenter Services, on page 136.

Structuring the Organization

This chapter contains the following topics:

Structuring the Organization

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 Service Catalog implementation:

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

Note   The Service Portal module prior to version 10.0 contained the My Workspace and System module page groups by default. These pages were obsolete in 10.x and will appear if Prime Service Catalog was upgraded from 9.x versions. As an administrator, you can disable these pages by removing the read permission of the page from the **Organization Designer > Roles > Anyone** role and the pages will be hidden from all users.

Accessing Organization Designer

The Organization Designer module is available with all installations of Service Catalog. 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 **Add** 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.

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 choose an entity of that type, control is 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 choosing the entity type to display. Once you have made your choice all entities of the specified type are shown in the content pane, below the search box. Search results display in alphabetical order.

- You can browse the list of entities in the content pane. As you move the mouse over each entity name, a hyperlink appears. You can click 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, choose the 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 appear— for example, entities whose names match a complete or full word entered. You can then browse those entities and choose 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.

Figure 4: Component search
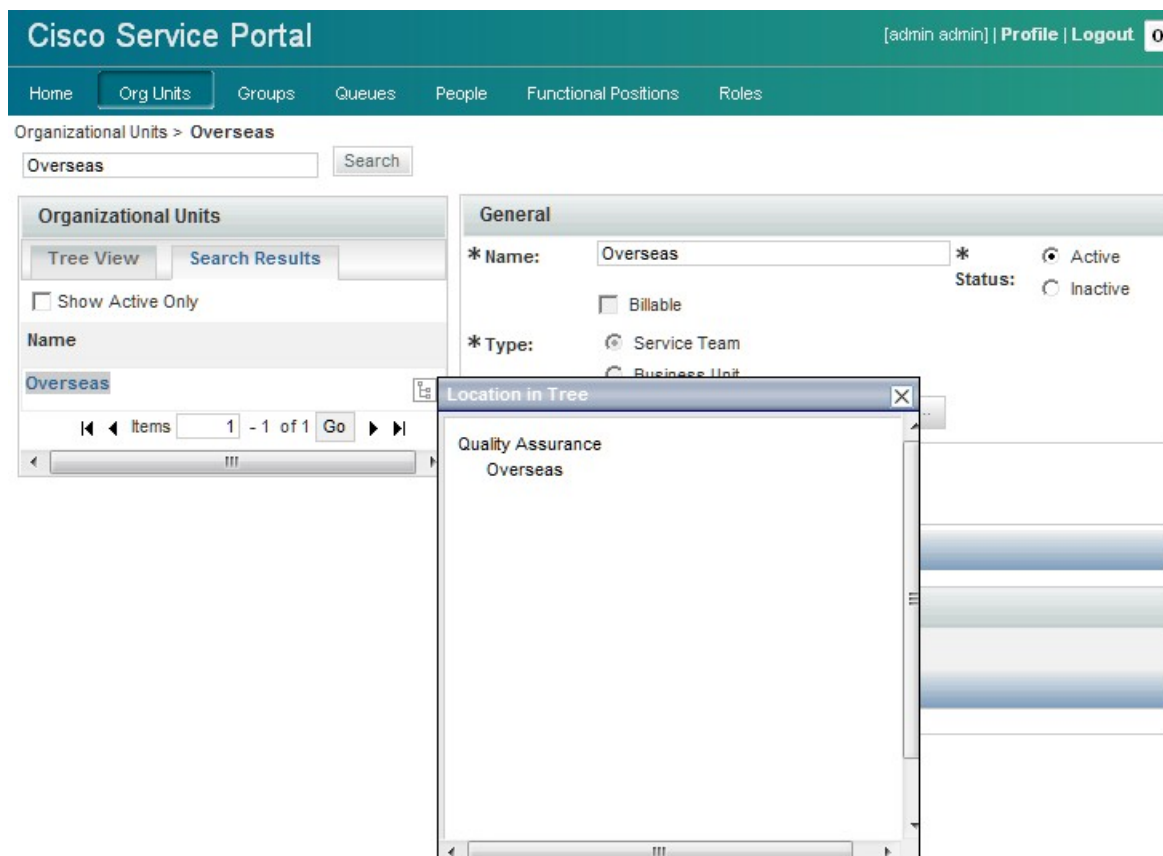
Maintaining Organizational Entities

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 choosing 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:

- From the Common Tasks page of the Organization Designer home page, click the **Create** link.

- Click the tab in the navigation pane corresponding to the type of entity to be created. Once the entity's home page appears, click **Add**.

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

This page typically includes all of the required attributes for creating the entity. Once you supply data for these attributes and click **Create**, the entity is 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 **Copy** 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 appear in any Search windows. For example, when a service designer attempts to assign a task to a particular queue, only active queues appear. 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.

Figure 5: Administration page
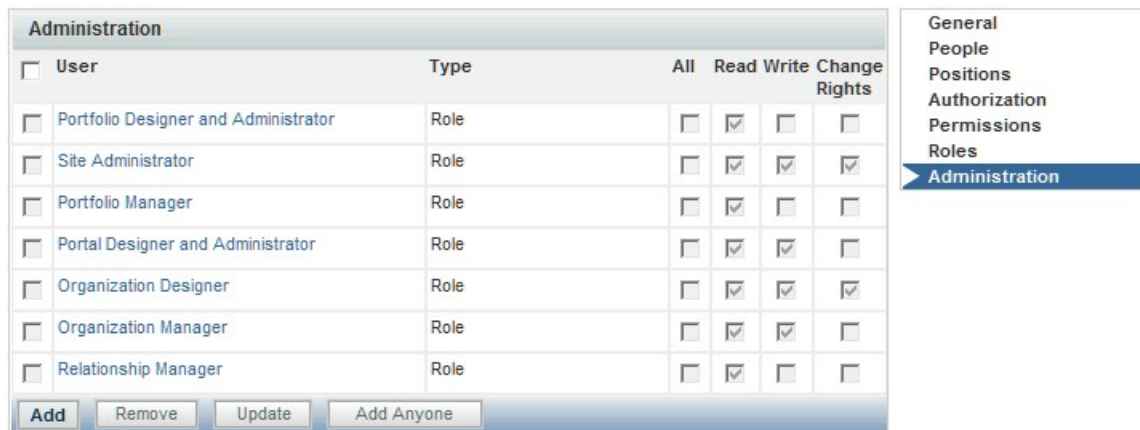
Administrative rights on an entity may be assigned to a specified organizational unit (hence inherited by all people in that organization unit), functional position, queue, group, or role. In addition, rights may be assigned to "Anyone" which means, any user who has the capability of accessing Organization Designer would be able to act on information on that entity. "Anyone". Anyone role with only read privileges will not be allowed to modify but just to read. This role should be added sparingly, if at all.

The following rights may be assigned:

Table 48: User Permissions

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 dimmed when the user does not have permission to change the rights.

System-defined entities are automatically granted predetermined sets of administrative rights. These entities are dimmed, 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 are able to access, and what capabilities they 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 Service Catalog 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 Service Catalog)

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 Catalog artifact, created so that a customized set of people are authorized to work on specific tasks. Therefore, the enterprise outside of the Service Catalog 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 Catalog from the directory. However, the directory in many cases does not hold such information, since roles and groups are typically Service Catalog artifacts, created expressly to facilitate usage of Service Catalog, 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 choose 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 is available for modification and entry of additional data as outlined below.

Table 49: Organization Unit page

Page	Description
General	General information about the organizational unit, including suborganizational 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 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 reactivated. Also, deactivating an organizational unit does not deactivate any queues associated with that OU.

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 suborganizational units.

General information about an organizational unit is summarized below.

Table 50: Organization Unit fields

Name	Name of the organizational unit
Status	Active or Inactive.

Name	**Name of the organizational unit**
Billable	**Note** This option is obsolete and not to be used. This will be removed in future. 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 choose a parent organizational unit.
Description	Any text describing the organizational unit.

Organizational Unit Hierarchies

Service Catalog 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 subOUs.

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.

- Suborganizational units can inherit roles and permissions from the parent, facilitating the assignment of responsibilities.

Suborganizational units, and therefore the members of that subOU, 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 suborganizational units to a parent, a helpful way to order your work is to:

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

Organizational Unit 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 OUs 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.
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 OUs 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 check box to the left of the queue/person's name is dimmed 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 nonhome OU.

To change the home affiliation for the entity, check the check 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 predefined 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, List-Bullet-Char1>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 **Assign**. A popup window appears allowing you to search for and choose the person or queue to be assigned.

An entity can be removed from a functional position by clicking **UnAssign**. 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 Setting up Site-Wide Authorizations, on page 202.

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 tree view in Service Manager.

To assign permissions for an OU, click **Add Permission** to display the Add Permission window. You then indicate which permissions 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.

Viewing Permissions

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 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. You can perform the following:

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 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.

Table 51: Configuring Group fields

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 subgroups.

Adding or Removing Subgroups

Subgroups 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 subgroups. subgroups are grouped within a parent group.

Subgroups, and therefore the members of that subgroup, 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-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 subgroups to a parent, a helpful way to order your work is to:

1 Create the subgroups.
2 Create the parent groups.
3 Add the subgroups to the parent group.

Members

Group members consist of a combination of organizational units and 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 checking the check box to the left of the member name and then clicking **Remove**.

Using Groups in Service Design

Permissions can be assigned to groups, rather than being assigned to individual people or to organizations. It is 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:

Table 52: Service Group fields

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 wish to grant that role.

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

Users and User Groups Imported from UCS Director

Note   In a single pane of glass, where Prime Service Catalog, UCS Director are connected to LDAP:

- The Home OU of a user is always determined by LDAP mapping .

- The User gets group membership of UCS Director if the user belongs to UCS Director imported groups.

- If the User data that is imported (discovered) does not exist in Prime Service Catalog, the same is created in Prime Service Catalog and the normal flow for OU, Group and Role is executed.

When Prime Service Catalog connects to a UCS Director for the first time, Prime Service Catalog creates a:

- **UCSD ::<ID>::All Groups:**

Where <ID> is the 3-letter identifier of the UCS Director server. This group will be the parent group for all groups imported from this UCS Director server.

- **UCSD ::<ID>::<Group Name>**:

Where <ID> is the 3-letter identifier of the UCS Director server. There will be group for each group in the UCS Director. All such groups are grouped under the parent group. Users belonging to various groups in the UCS Director are imported to the respective groups in Prime Service Catalog.

- **Default group**. The default group is grouped under the parent group. Users without a group in the UCS Director are imported to this group.

All the imported users from the UCS Director are assigned an Organizational Unit (OU) in Prime Service Catalog.

During the subsequent connections, Prime Service Catalog checks for group membership changes and updates the records accordingly.

Note   For container templates, container catalogs, standard catalogs, and advance catalogs services created in Prime Service Catalog for UCS Director:

- If these services are associated to a group in UCS Director, users in the corresponding group in Prime Service Catalogs can only order services that the group has access to.

- If the services are associated to All Groups in UCS Director, users in the corresponding group in Prime Service Catalog can order the services that All Groups have access to.

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 Catalog comes with one preconfigured 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 is placed in the Default Service Delivery Queue.

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

Table 53: Queue page fields

Page	Description
General	General information about the queue
Org Units	Organizational units assigned to the queue
Contact	Contact phone numbers 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 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. Service Catalog 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

This section describes about how to configure the 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.

Table 54: Queue fields

Page	Description
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 appears, 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.

Associating Queues and Organizational Units

You can specify the service teams 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.

Administrators may refer to queue contact information if a problem arises with delivery of tasks assigned to a particular queue. Different contact types (email, phone numbers, and so on) are provided. Multiple email addresses can be entered in the Email field in Queue Contact. The email addresses need to be delimited by a semicolon (with no spaces); for example, joe@cisco.com;dave@cisco.com.

All contact types except Email can be deleted from the queue contact information.

Setting Work Hours

Use the Calendar page to set the work hours and days, and assign nonwork 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.

- Enter times for the From and To fields, using a HH:MM AM/PM format.

- Enter 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. Click **Add New** to add a new date. Enter the date by choosing 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 preconfigured roles automatically can access any queue. Consequently, any entity (person, organization, or group) granted one of those roles is 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 Service Catalog 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.

Adding a Person

Service Catalog 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 Prime Service Catalog Integration Guide.

• The Directory Task available in the service workflow (delivery plan) can create a person based on service form data. For more information, see the Cisco Prime Service Catalog 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 (marked with an asterisk (*)):

Table 55: People fields

Page	Description
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 that appears 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 choose 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, reenter 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:

Table 56: People fields

Page	Description
General	General information about the person.
Org Units	Organizational units to which the person belongs.
Address	Company or personal address information.
Contact	Contact phone numbers 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.

Page	Description
Administration	Entities with permission to view 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:

Table 57: General fields

Field	Description
Title	Abbreviation used when addressing correspondence to the person; Ms. or Mr., for example.
IsLocked	If a user's account is locked due to password expiration or retry policy violation, the IsLocked field is enabled automatically. To unlock the user account, disable the IsLocked field and then reset user password. For more information about resetting a user's password, see LoggedIn User Password field in General Person Information, on page 161.
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 that appears on the user interface for the person.
Employee Code	Company-derived employee code, if any.

Field	Description
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.
Authenticate Yourself Before Changing Password	A user's password must be reset if the account is locked due to the violation of one of the following policies:
	• Password expiration policy
	• Retry policy
	The administrator has the privileges to reset a user's password. To do so, the application ensures that the logged in user is authenticated to change the password of another user.
	After the logged in user credentials are authenticated, the logged in user, that is the administrator can change the user password using the Login, Password, and Confirm Password fields.
	Note • If you change your password, you are automatically logged out from the system. A popup window appears, prompting you to log in using the new password. • If External User Authentication (EUA) is not enabled or if you are using a Site Administrator URL the authentication for password change must be the local application password of the logged in user trying to change the password. If EUA is enabled you must use the LDAP password in this field.
	For more information about password policies, see Password Policies, on page 227.
Login	A unique login identifier.
New Password	The password used to log on to the system.
Confirm Password	Reenter the password.

Figure 6: General page

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 choose 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 requester 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 email, telephone, and so on.

- 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.

- All contact types except email address can be freely added to and deleted from the person's contact information.

Adding Additional Information using 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 appears 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 attributes 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 Catalog 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 preconceived semantics. If you have additional personnel information in the LDAP directory that needs to be exposed in Service Catalog, 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, enter times for the From and To fields, using a HH:MM AM/PM format.

- Enter 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** link 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 chosen person:

The Permissions page also designates the Authorization Delegate for the chosen 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.

Table 58: Authorization Delegate fields

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

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 reactivated.

Once a person has performed any activities within Service Catalog, 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 Catalog application. A task within the system can be assigned to a functional position. A person, 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 the four entity types:

- Organizational Units
- Service Groups
- Services
- Accounts

Service Catalog provides several standard functional positions, which cannot be modified. In the illustration below, the check boxes to the left of the system-defined functional positions are dimmed, indicating that these positions cannot be deleted or updated. The "Manager" and "Tester" positions were created at this site.

Figure 7: Functional positions page
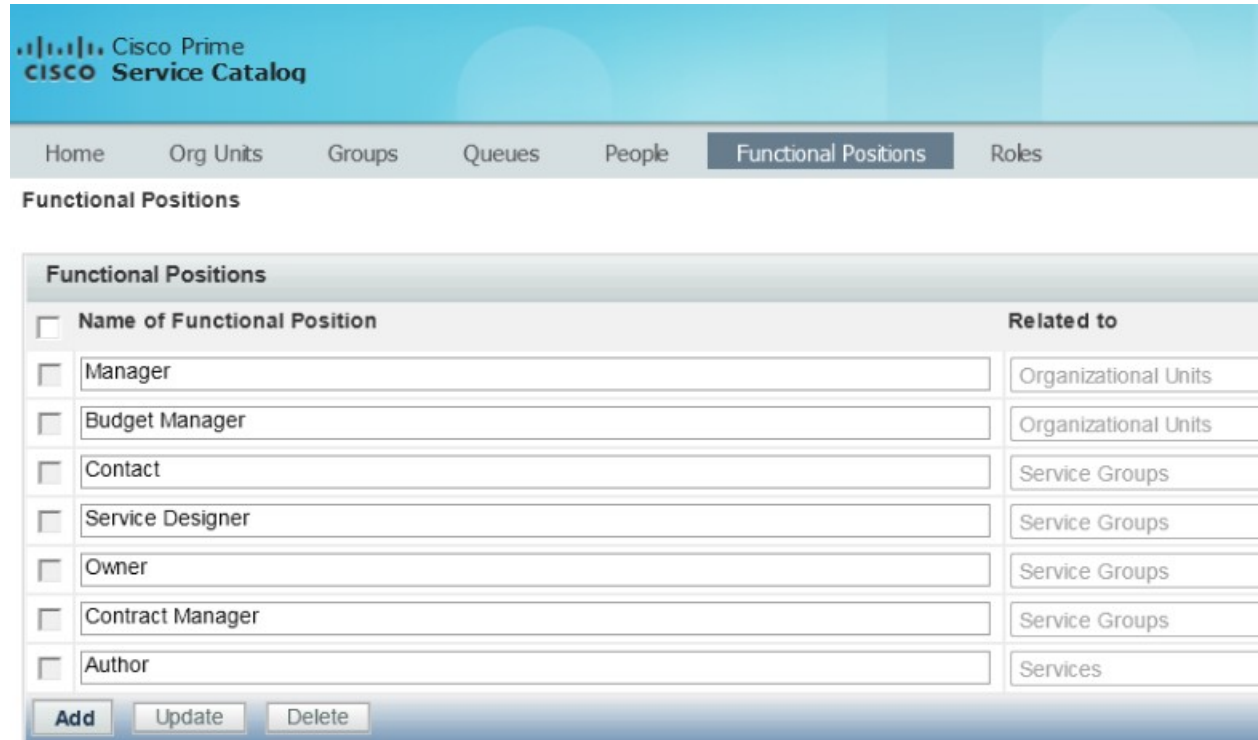
Functional positions associated with each type of entity appear on the Positions page for organizational units in Organization Designer, or on the General tab for services or service groups in Service Designer. For example, with just the standard functional positions associated with an organization, the account functional positions page for maintaining Organizations would look like this:

Figure 8: Positions page
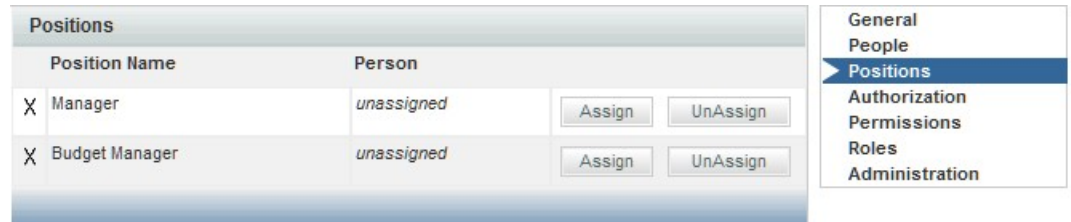
Creating a Functional Position

If the system-defined functional positions do not meet your company's requirements, you can create functional positions. To add a new functional position:

Step 1   Click **Add** on the Functional Position page, a new line will appear at the bottom of the list of positions.

Step 2   Enter a name for the functional position and choose its **Type** from the drop-down menu on the right.

Step 3   Click **Update** to save the new functional position. The name cannot be the same name as a previously defined functional position even if it has a different Type. Also, the name should not contain spaces, even though this is permitted. A name with embedded spaces cannot be used as a namespace variable.

Step 4   By choosing the **Type**, you associate the position with an organizational unit, service group, or service. New functional positions associated with each type of entity are automatically added to the Positions page for organizational units in Organization Designer, or on the General tab for services or service groups in Service Designer.

Once the functional position has been defined, you may assign a person to the position through the Positions page for the organizational unit in Organization Designer, or on the General tab for the service or service group in Service Designer.

Modifying a Functional Position

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

- The standard positions display a disabled (dimmed) 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 name.

- You cannot update a position association (Type). 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 dimmed check box. 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 **Delete**.

Roles

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

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

When an organization is created, it is automatically granted the My Services Consumer role. This allows any members of the organization (or suborganizations) 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 Service Catalog, both default roles provided by Service Catalog and custom roles created in each installation can be granted to an organization. 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. See the Cisco Prime Service Catalog Designer Guide for more information on setting entity protection levels.

You can download the detailed list of all the out-of-box RBAC roles and capabilities here.

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.

System-Defined Roles

- Table 59: ITIL- Based System Defined Roles, on page 170

- Prime Service Catalog System Defined Roles for UCS Director Integration, on page 126

Service Catalog 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. 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.

Table 59: ITIL- Based System Defined Roles

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

Role Containers	Description		Roles
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.		
	Subcontainers	**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

Role Containers	Description	Roles
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 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 Catalog Management Roles	Roles supporting the processes of defining and managing the Service Catalog.	• Distributed Portal Designer • Portal Content Provider • Portal Designer and Administrator

Role Containers	Description	Roles
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 Catalog.

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 Catalog would be able to perform the functions provided by those roles and capabilities.

The "Site Administrator" role, 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 Service Catalog 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.

Prime Service Catalog System Defined Roles for UCS Director Integration

Prime Service Catalog creates the following system-defined roles for the UCS Director roles it discovers. The following table lists the mapping of the UCS Director to Prime Service Catalog system-defined roles.

Table 60: Prime Service Catalog Roles Mapping with UCS Director Roles

UCS Director Roles	Prime Service Catalog System Defined Roles	Description
System Admin	UCSD Sys Admin	UCSD Sys Admin user can view the details of Containers, vDC's and VM's as service items in My Products and Services based on the Group permissions assigned to each of the UCS Director Service Item in Service Item Manager.
All Policy Admin		
Computing Admin		Only users with this role can order Container Template Services.
Service End-User, Group Admin, Operation roles	UCSD End User	UCSD End User can view the details of Containers, vDC's and VM's as service items in My Stuff based on the Group permissions assigned to each of the UCS Director Service Item in Service Item Manager.
		Users with this role can order services based on the group to which user belongs and catalogs which are assigned to a group in UCS Director.
All other roles	UCSD Operator	Users with this role can only view and use the self-service portal but cannot order the services.

Note   In a single pane of glass, where Prime Service Catalog, UCS Director are connected to LDAP:

- The Home OU of a user is always determined by LDAP mapping .

- The User gets group membership of UCS Director if the user belongs to UCS Director imported groups.

- If the User data that is imported (discovered) does not exist in Prime Service Catalog, the same is created in Prime Service Catalog and the normal flow for OU, Group and Role is executed.

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.

Figure 9: Roles page
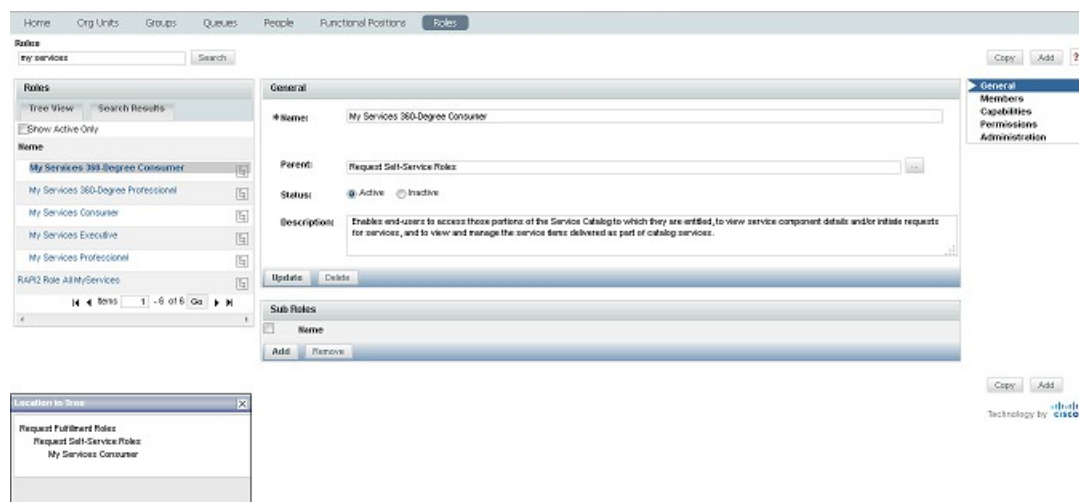
In the example above, "My Services Consumer" was entered into the Search field. The role was found and listed on the Search Results tab. You can see, by clicking the hierarchy icon, that this role resides in the Request Fulfillment Roles container, which resides in the Request Self-Service Roles container.

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:

Table 61: Roles fields

Page	Description
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.

Page	Description
Capabilities	Capabilities included in a role. You cannot add or delete capabilities in a system-defined role, although you can add subroles/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. You can choose to select all objects or specific objects.
Administration	Entities with permission to view 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, suborganizational units and subgroups inherit roles from their parent. The **Show inheriting members** option allows you to choose whether to show those members who have inherited the role from a parent organizational unit or group. If not checked, only organizational units and groups directly assigned to the role appear.

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.

Figure 10: Members page

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.

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:

Figure 11: Capabilities page

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.

Figure 12: Permissions page

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.

Step 1   Create this role by doing one of the following:

  • Create a new role.

  • Copy a similar role to use as a template for a new role.

Step 2   Make the user-defined role a child of a system-defined role.

Step 3   Define the new role by adding capabilities and permissions as needed.

Step 4   Assign members to the role.

General Role Information

Enter the following information:

Table 62: Add Role fields

Page	Description
Name	Name of the new role.
Parent	Click the ellipses … to search for and choose 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

A "capability" is the ability to perform certain functions within Service Catalog. It is critical to review the capabilities that are available and how they are combined in the predefined roles in order to be able to assign the predefined 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 that appears. Capabilities are divided by module, since each capability confers rights to perform functions within a particular module.

To disable the access provided to the roles, remove the role from the selected person or remove the capabilities that was assigned.

Capabilities for each module are summarized below.

Capabilities for My Services, Service Catalog, and Order Management

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

Table 63: My Services Capabilities

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 Percentage Completion of Requisitions	This capability allows the user to see the requisitions completion percentage. You can enable the percentage display in Service Catalog > My Products & Services > Orders page by setting the `servicecatalog.display.req.percentage.completion` property in the newscale.properties file to true. **Note** You must restart Service Catalog server every time you modify the newscale.properties file.
See Requisitions for My Business Units	Users with this capability can see all requisitions for their business units in the My Stuff view.
View and Perform Authorizations	This capability controls whether users can see the "Authorizations" link in the top navigation bar.

Capability	Description
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	Users will see the Order on Behalf link in the top level navigation bar if you they are using the My Services module. 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.
Access Service Item Instance	This capability enables the user with this role to view the My Products &Services section in Service Catalog module. users who use My Services will be able to access "**Service Items**" tab in **My Services** module.

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

Most of these same capabilities govern the equivalent functionality in the Service Catalog and Order Management modules. The only exception is "View KPIs" which is not available outside of My Services. There are also some differences in how some of these capabilities work in Service Catalog. Users who have

chosen Service Catalog as their catalog view will have implicit capabilities for service browse and search, and use the "Order for others" action buttons to order services on behalf of another person.

Table 64: Service Designer Capabilities

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.

Capability	Description
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.

Table 65: Service Link Capabilities

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.

Table 66: Reporting Capabilities

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.
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 such as manage Reporting folders, dashboard, IBM Cognos Administration, schedule reports, save reports, permissions administration, and create reports.
View Service Catalog Reports	This capability grants access to the Reporting module and the ability to view the KPI dashboard and run Service Catalog 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.

Table 67: Service Manager Capabilities

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 Tasks2. Close Out Tasks3. Standard Views4. Cancel Tasks for which they are the Task Supervisor
Manage Work	Users have access to the following system behaviors:1. Assign Work2. Set Task Priorities 3. Reschedule Task Due Dates4. Administration View5. Service Teams View

Capability	Description
Perform Global Delivery Search	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 Prime Service Catalog Integration Guide and performing Directory Tasks (described in the Cisco Prime Service Catalog Designer Guide). Together with object-level permissions, allowing users to read and write specific organizational entities, the capabilities provide granular control over a multi tenant environment.

Table 68: Organizational Designer Capabilities

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.

Capability	Description
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.

Table 69: Administration Capabilities

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 can view and download log and property files.
Access Purge Utilities	Users see the Purge Utilities tab and can use purge utilities.
Access Version History	Users see the Version History tab and can view version history.
Access Form Data Viewer	Users see the Form Data Viewer tab and can use the Form Data Viewer.
SAML SSO Settings	User see the SAML SSO Settings tab and can perform the CRUD operations for IDP Mappings, SAML Configuration and perform the Refresh Metadata.

Capabilities for Catalog Deployer

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

Table 70: Catalog Deployer Capabilities

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 Service Item Manager

Standard roles relating to Service Item Manager and the capabilities included in each are summarized in the table below.

Table 71: Service Item Manager Capabilities

Capability	Description
Manage Standards Definitions	This capability enables the user assigned to this role to define and manage standards, including adding and deleting entries
Manage Service Item Definitions	This capability enables the user assigned to this role to define new service items and their attributes
Import Service Item and Standards Data	This capability enables the user assigned to this role to access the import options to import service item and standards data and definitions
Access Service Item Instance Data	This capability enables the user assigned to this role to access "**Manage Service Items**" tab in **Service Item Manager** module.

Capability	Description
Access Service Item Definition	This capability enables the user assigned to this role to access "**Design Service Items**" tab in **Service Item Manager** module.
Access Standard Data	This capability enables the user assigned to this role to access "**Manage Standards**" tab in **Service Item Manager** module.
Access Standard Definition	This capability enables the user assigned to this role to access "**Design Standards**" tab in **Service Item Manager** module.

Capabilities for Portal Designer

Capabilities for using Portal Designer are described in detail in the 'Designing Portals' chapter, of the Cisco Prime Service Catalog Designer Guide .

Capabilities for Localization

Adding the **Localization Management** capability allows a user role to access the Localization module.

Capabilities for SOAP-based Services through API

In addition, users will be able to submit requisitions through Service Catalog, which provides the ability for external systems to submit requisitions through a web service request, using the SOAP-based version of Requisition API (RAPI). Users can also request using the REST-based API. Such requests, bypassing the Service Catalog module, would never have a service form appear 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 Java Script 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 through RAPI. Such services should never appear in the Service Catalog of nonadministrative 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.

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:

Table 72: Assigning Permissions

Module	Objects	Permission
Service Designer	Service Group	• Design services and change data in this service group: Allows the user to create new services, and view/modify existing services contained within the service group. The set of Service Designer tabs that are visible depends upon the particular capabilities granted. If the Permissions tab is visible, it is not editable unless the user also has the "Assign Rights" permission to edit it. • View services and other information in this service group: Allows the user to view the service group and the services contained within the service group in Service Designer. The set of Service Designer tabs that are visible depends upon the particular capabilities granted. • Order service group services: Allows the user to view and order services in the service group within My Services portal. A service must also be defined as Orderable to be able to order it. • Assign rights: Allows the user to access the Permissions tab on the service group and service pages. The user must also have either "View services and other information.
	Service	Order Service: Allows the user to view and order the service within My Services portal. The service must also be defined as Orderable to be able to order it.

Module	Objects	Permission
	Form Group	• Design forms in this form group: Allows user to create new and view and modify existing Forms contained within the Form Group. All tabs are editable (including the Permissions tab). • View forms in this form group: Allows user to view the Form Group and the Forms contained in it.

Module	Objects	Permission
Organization Designer	• Person • Organizational Unit • Queue • Role • Group	• Read: Allows the user to view all pages of the object record with the exception of the Administration page. • Read/Write: Allows the user to view and edit all pages of the object record, with the exception of the Administration page. • Change Rights: Allows the user to view and change the permission rights on the Administration page of the object record. • Order on Behalf: Users with this permission are able to use the Order of Behalf feature of My Services for this object. • Manage Service Team: Users with this permission are able to see the Service Team OU in the Service Team view within Service Manager. **Note** This permission is available only for Organizational unit object. • Access Queue: Users with this permission are able to see and work tasks in the queue within Service Manager, given their capabilities defined for the Service Manager module. **Note** This permission is available only for Queue object.

Module	Objects	Permission
Portal Designer	• Portlet • Portal Page	• Read: Allows the user to view the object (portlet/ page) definition in Portal Designer. • Write: Allows the user to edit the object (portlet/ page) definition in Portal Designer.
	Portal Page Group	• Read: Allows the user to view the page group definition in Portal Designer. Also allows the user to view the page group in the form of a menu option in Service Catalog if the page group is marked as a Module. • Read/Write: Allows the user to edit the page group definition in Portal Designer. Also allows the user to create portal pages in the group in Portal Designer and Service Catalog. • Read all pages in the group: Allows the user to view all the pages in the page group in Portal Designer. Also allows the user to subscribe to all active public pages in the page group in Service Catalog. • Write all pages in the group: Allows the user to edit the definition of all the pages in the page group in Portal Designer and Service Catalog. Also allows the user to create portal pages in the group. **Note** Portal pages are available in Service Catalog only if they are marked public.

Module	Objects	Permission
	Custom Content	• Read: Allows the user to view the content definition. Also allows the user to view the custom content definition when it is rendered in portlets in Service Catalog. • Read/Write: Allows the user to edit the content definition. • Read Data: Allows the user to view the content data and the associated definition in Portal Designer. Also allows the user to view the custom content data when it is rendered in portlets in Service Catalog. • Read/Write Data: Allows the user to edit the content data.
	Custom Content Group	• Read: Allows the user to view the content group and create content definitions in the group. • Read/Write: Allows the user to edit the content group and create content definitions in the group. • Read all definitions in the group: Allows the user to view all content definitions in the group and create content definitions in it. • Read/Write all definitions in the group: Allows the user to edit all content definitions in the group.
Demand Management	Billing	Maintain Billing Rates: Allows the user to manage billing rates.

Module	Objects	Permission
Service Item Manager	• Service Item Definition • Service Item Group • Standard Definition • Standard Group	• Read: Allows the user to view object. • Read/Write: Allows the user to edit object such as performing CRUD operations
	Service Item Instance Data	

Module	Objects	Permission
		• Read all Instance Data: Allows the user to view all service item instances.
		• Read/Write all Instance Data: Allows the user to view and edit all service item instances
		• Read all Instance Data in my BU: Allows the user to view all service item instances that is assigned to his business unit (BU)
		• Read/Write all Instance Data in my BU: Allows the user to view and edit all service item instances that is assigned to his business unit (BU)
		• Read all Instance Data in my BU and their sub-units: Allows the user to view all service item instances that is assigned to his business unit (BU) and its sub units
		• Read/Write all Instance Data in my BU and their sub-units: Allows the user to view and edit all service item instances that is assigned to his business unit (BU) and its sub units
		• Read all Instance Data in my Tenant Account: Allows the user to view all service item instances that is assigned to his tenant account
		• Read/Write all Instance Data in my Tenant Account: Allows the user to view and edit all service item instances that is assigned to his tenant account
		• Read all Instance Data in my Project Account: Allows the user to view all service item instances that is assigned to

Module	Objects	Permission
		his project account • Read/Write all Instance Data in my Project Account: Allows the user to view and edit all service item instances that is assigned to his project account • Create New Instance Data: Allows the user to create new service item instance data. **Note** Users are provided read access to the service they are subscribed to by default.
	Standard Table Data	• Read all Instance Data: User can view all the standard instance data. • Read/Write all Instance Data: User can view and make changes to all standard instance data. • Create new standard instance data: User can create new standard instance data.

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

Table 73: Object-level Permission

Page	Description
Object Type	Choose an object (entity) type from the list box.
Permission for this type	Based on the object type selected, choose the permission.

Page	Description
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 choose the objects to which you wish to assign this permission.
	The following additional permissions are applicable for person - object type and for read and read/write permission types only:
	• ◦ All people in the Organizational Unit and its sub-units of which user is a member – The person assigned to this role gets access to read or read /write information about all people from the OU he belongs to and all people belonging to its sub OUs
	◦ All People in Organizational Units of which user is a member– The person assigned to this role gets access to read or read /write information about all people from the OU he belongs to.
	◦ All people that belong to the person account – The person assigned to this role gets access to read or read /write information about all people from the account he belongs to.
	The following additional permissions are applicable for organization unit- object type:
	• ◦ All Service Teams of which user is a member
	◦ All Service Teams

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.

Assigning Permissions to People with Custom Roles

You can assign read or read/write permissions to people with custom-defined roles such that he could view or make changes to a limited set of people. In this scenario, you configure permission for a user such that, the person with the defined custom role will be able to view accounts of all people who belong to the same account as he is.

To add permissions to people with custom roles:

Step 1 Choose **Organization Designer** > **Roles**.

Step 2 Select a role from the Role Hierarchy pane.

Step 3 Click **Permissions**, in the list panel to the right-side of the screen.

Step 4 Click **Add Permissions** in the Permission Assigned to this Role table.

Step 5 In the Add Additional Permissions pane select:

- ◦ **Person** in the Object Type drop-down list.

  ◦ **Read** in the Permissions for this type drop-down list

  ◦ Click All people that belong to person account

Step 6 Click **Add**.

You can view the people with access permission you provided in the following modules:

- Organization Designer > Home > Search > People

- Profile > Preferences > Authorization Update > Select Person

- Service Designer > Services > Form

Usage Scenarios to Create Sample Custom Roles

This section describes the various scenarios for the 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.

To create a role for the support team:

Step 1   Create a new role.

Step 2   *Add the capability* **Perform Global Delivery Search** *listed in the Service Manager module* . This will allow any member of this role to access the Service Manager module and search for all tasks/requisitions.

Step 3   Assign your support team as members of this role. For more information, see Assigning Members to a Role, on page 176.

Organization-Specific Service Team Administrator

The "Service Team Administrator" preconfigured 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 Service Catalog requisition that includes an integration to Remedy, and may need, for example, to add attachments or comments to such requisitions.

Step 1   Create an OU of type = Service Team, named, for example, **Remedy Team**.

Step 2   Make all the people who need access to these requisitions members of this OU.

Step 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.

Step 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 is why this works: Service Catalog 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 Service Catalog 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. However developers must ensure that they do not accidentally or on purpose change 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 groups

- 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 preexisting 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.

APPENDIX **B**

Configuring Site-Wide Settings

This chapter contains the following topics:

Configuring Site-Wide Settings

Overview

You can set up a variety of behaviors in the Administration module to accommodate the rules and business practices of your company.

You can perform the following tasks through the Administration module:

- 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 style sheets to be used by specific organizational units or groups of those units.

- Access support utilities for log files, purging, version information, and viewing form data.

Synchronizing User Information

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 Prime Service Catalog Integration Guide.

Setting up Site-Wide Authorizations

You can enable or disable authorizations and reviews, and set up site-wide authorizations using the Authorizations tab of the Administration module. Such site-wide authorizations can be used in addition to, or instead of, authorizations established for individual organizations and services or service groups.

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.

Service Catalog supports several types of authorizations and reviews.

Table 74: Authorizations

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 Authorization Structure

Setting up an authorization process consists of three steps:

1 On the Authorizations tab of the Administration module, specify which types of authorizations are available, and the order in which they should be performed. (See Enabling Authorizations, on page 202.)
2 Specify the details for each type of authorization which has been enabled. (See Specifying Authorization Details, on page 203.)
3 Optionally specify the escalation procedure to be followed if a required authorization is late. (See Notifying Delayed Tasks, on page 206.)

Enabling Authorizations

Up to five authorization types can be enabled for a site on the Authorizations tab of the Administration module.

To change the status of an authorization type, under the Action column for the authorization type you want to change, click **Edit** and choose **Enable** or **Disable** from the Status drop-down menu. To change the order of execution, in the Action column click the Up or Down Arrows 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 (**Administration > Authorizations**)

- For each organization for Departmental Authorizations/Reviews (**Organization Designer > Org Units > Authorizations**)

- For a service group or service for Service Group Authorizations/Reviews (**Service Designer >Authorizations**)

For Departmental Authorizations/Reviews you have the option to:

- Use site authorization structure only

- Use departmental level authorization only (Will not use site level)

- Use both site and departmental level authorizations structures

For Service Group Authorizations/Reviews you have the option to:

- Use service group authorization structure only

- Use service level authorization only (will not use service group-level)

- Use both service group level and service level authorizations structures

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

- An Authorization (Departmental or Service Group) – 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 canceled, no further tasks are performed.

- A Review (Departmental or Service Group) – 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.

On the Authorizations tab of the Administration module, in the Actions column next to the authorization or review you want to edit, click **Edit**. Based on the authorization type you choose, either the Authorizations – Sequential Process or Reviews – Concurrent Process subtab appears.

This following table defines the fields on the Details screen (which appears after you click **Add** on one of these subtabs, or choose a previously defined authorization/review role by checking the check box to the left of the Name field in one of these subtabs). Click **Update** to save changes. Fields marked with an asterisk (*) are required.

Table 75: Sequential Process - Authorization

Field	Description
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 Prime Service Catalog 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	Choose 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	Choose one of the following from the drop-down menu: • From a position – authorization or review is fulfilled by the person currently filling the designated functional position • A person/queue – authorization or review is fulfilled by the designated person or queue • From an expression – authorization or review is fulfilled based on the expression entered in the "Assign to" field
Assign to	Click […] to choose the value that corresponds to your selection for the Assign field. If you choose **From an expression**, enter the expression. Expression syntax is documented in the Cisco Prime Service Catalog Designer Guide.

Field	Description
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. • Task becomes active (times will not be affected, scheduling is done by using these efforts) – The condition entered in the Condition field becomes active when the authorization phase completes and the task after the authorization begins.
Re-evaluate expression as authorizations/reviews proceed	Check the check box 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.

Field	Description
Notify when authorization/review starts	Email templates are automatically sent at every phase appropriately. A list of email templates available in the system is displayed in the drop-down list.
Notify when authorization/review completes	
Notify when requisition/activity is canceled	
Notify when requisition/activity is rejected	
Notify when task is rescheduled	
Notify when task is reassigned	
Notify when external tasks fail	

Notifying Delayed Tasks

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

When setting up an escalation process, note 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 choose 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 is 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. For details, see Maintaining Prime Service Catalog, on page 5.

Email Templates

Service Catalog includes a set of preconfigured email templates. You can set up a delivery plan of a service 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 email are used to inform recipients of steps within the approval and delivery process.

Templates used by Service Catalog 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 Service Catalog template is shown below.

Figure 13: Email Templates page

Configuring Templates

To configure an email template, supply the following information:

Table 76: Email Template fields

Field	Description
Name	Name of the new email template.
Subject	email subject; may use namespaces.
From	Sender's valid email address.
To	Valid email address for recipients; multiple recipients can be separated by semicolons; typically uses namespaces.
Type	Service Catalog or Demand Center.
Language	Display language.
HTML Part	Click to show the template as it would appear in an HTML-aware email system. When clicked, HTML Editor tools appear 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. Preconfigured templates cannot be deleted.

Service Catalog 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, see the Cisco Prime Service Catalog Designer Guide .

Using Namespaces

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

The recipients of the notification 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.

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:

Table 77: List fields

List name	Description
Cost Drivers	Cost Drivers are available when configuring Cost Details for services in Service Designer.
Objectives	The Objectives list is used to configure Objective Metrics that are available in a drop-down list when creating Objectives in Service Designer.
Unit of Measure	Units of Measure are used in conjunction with Metrics to configure Objectives in Service Designer.
Language	The Language list is used to manage the list of languages that are available for users to choose in the Preferred Language drop-down list in the user profile and in the person information. For more information, see the Language, on page 210.

Language

The Service Catalog module is available in multiple languages. The Language list is used to manage the list of languages which are available for users to choose in the Preferred Language drop-down list in their Person Profile (see the Language Settings, on page 1). 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, choose the language from the drop-down list, and then click Update. No additional configuration steps are required.

For Service Catalog, the supported languages are as follows:

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

For localization of all other modules, see 'Localizing Service Catalog Strings' chapter in Cisco Prime Service Catalog Designer Guide .

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:

Table 78: Site Settings page

Page	Description
Customizations, on page 211	Configure site-wide settings for various modules.
Person Popup, on page 224	Set the type of information that displays when conducting a person search.
Entity Homes, on page 225	Specify the definitional data that can be modified on the sites of an implementation.
Application Locale, on page 226	Ensure that all new users use the updated language and the corresponding currency.
Password Policies, on page 227	Define policies for configuring passwords.
Debugging Settings, on page 234	Specify whether to display debugging information within the user interface.
Data Source Registry, on page 235	View the data sources registered with the application.
Custom Themes, on page 251	Define and specify the organizations to which they apply.
Public and Private Keys, on page 235	Configure public and private keys for AMQP.

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:

Table 79: Customization

Show Resource String ID	Controls whether the string IDs are displayed alongside the product and content strings. This setting is useful when performing string localization or translation.
KpiSourceOfData	Controls where the KPI charts retrieve data. Should be set to "Datamart".
SessionTimeOut	Sets the session time out; default is 20 minutes; may be any interval up to two hours (240 minutes).
API SessionTimeout	Sets the session Timeout for all APIs. If any nsAPIs are directly called with credentials (without calling nsAPI login) then the Session should be automatically terminate after the response is sent.
Fiscal Year End	Sets the month and day of fiscal year end for fiscal calendar related calculations.
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.
Image Maximum Size	Sets the maximum size of the file that can be uploaded as an attachment 0 indicates no maximum size.
Image Types Allowed	Defines the image types that are allowed. Specify these as a list of file extensions separated by comma. For example: .jpg,.img,.bmp. By default, the following images types allowed: .jpg,.png,.gif,.jpeg,.tiff,.exif,.svg
Order Confirmation Email Template	Email notification to be sent when a customer submits a requisition.
Order Failure Email Template	Email 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	Email 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 results returned by non-directory-enabled person popup	Maximum number of people returned when end-users attempt *select (*)* type queries in non-Directory-enabled Person Popup dialogs by entering only wildcard characters (default is 1000 people; 0 indicates all people).
Mail Server Address	Set host name of server used for e-mail communication. Host Name, Port and Support Email Address are mandatory to test connection.

Mail Server Port	Port used for communication by mail server.
Support Mail Address	Email address of support team.
Browser Cache Version	The Browser Cache setting enables the browser-side caching of images, JavaScripts, css, and so on, which may improve performance. When the Version setting value is incremented, the login process is interrupted until the browser's cache is deleted. Default is Disabled.
SDP Admin UserName	Enter Base URL in the Format of HostName and PortNumber.
SDP Admin Password	
SDP Host and Port	
JMS Username	Enter the JMS username and password values that are first captured when the application is installed. Subsequent changes to the credentials on the application server side (as necessitated by corporate password policies or other requirements), the updated values need to be entered here to allow the Prime Service Catalog application to continue to have access to the JMS queues.
JMS Password	
Audit History Retention Period	Sets the period for which the Audit history data is retained. The default value for retention period will be 60 days. The minimum will be 1 day and maximum will be 365 days. When Prime Service Catalog is upgraded to a newer version the audit history data will be retained after upgrade if the data falls within the retention period specified. Based on the retention period specified in the **Administration > Customizations**, system will check for the records older than the specified duration and will delete those data from audit history tables. By default, the scheduler processes the older data once in every week. You can modify the duration of the scheduler in the **newscale.properties** file."
Maximum number of saved views in MyStuff	Sets the maximum number of views that can be saved by users in MyStuff. Minimum allowed value is 5 and maximum allowed value is 20.
Service Catalog search pagination size	Sets the maximum number of records, which can be returned using the search services functionality. This search functionality allows infinite scroll, owing to which end users need to simply scroll down to trigger the next search. The minimum and maximum values allowed are 20 and 50, respectively.
My Stuff Default View	Sets the default view for all users in My Products & Services who do not have a default named view. The default view set by the administrator can be overwritten by the users in My Stuff with their own named view.
Path of the folder containing the FTL Files	Mention the fully qualified path name of the folder containing the FTL templates for VDC-based email notification. The file path should be in Linux convention, which uses / as the file separator.

Asynchronous Submission/Last Approval

In order for Service Catalog 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 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 acknowledgment that their attempt to submit the service request has been processed.

To eliminate this wait time, Service Catalog 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 Catalog 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—are performed asynchronously, in the background.

This results in one major change in the user interface (elimination of the wait time!) and some minor changes. After requisition submission, the status becomes "Ordered" until it is processed by the Business Engine. Afterwards, the status becomes "Ongoing".

In the rare case when Service Catalog 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 > Settings > Customizations** settings. Failed requests can be viewed and sent for retry on the Administration Debugging page. See the Monitor for Asynchronous Submission Messages, on page 235 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 **Administration > Settings > Customizations**.

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 allows the application to make use of the cached version of the following types of objects:

- Images (*.gif, *.jpg, *.png, *.bmp)
- 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 "Login Again" (or "Continue", when Single Sign-On is enabled) to access the application.

JMS Credentials

The JMS username and password values are first captured when the application is installed. Subsequent changes to the credentials on the application server side (as necessitated by corporate password policies or other requirements), the updated values need to be entered here to allow the Prime Service Catalog application to continue to have access to the JMS queues.

Common Settings

The Common Settings affect the behavior of multiple modules.

Table 80: Common Settings

Enable Custom Header Footer	Enable custom header and footer. Default is off.
Enable Custom Style Sheets	Use a custom style sheet for formatting the site, allowing for the changing of logos, color schemes, fonts, and other HTML attributes. Default is off.
Enable Custom Styles for Login Logout	Use custom styles for formatting the login and logout screens, including the labels such as username and password, allowing for the changes in font and size. 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.
Use Image Path Replacement	Use a dynamic variable in place of the server portion of presentation image URLs. 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.
Accept encrypted Password	When enabled, the password used for inbound HTTP requests must be in encrypted format. Default is off.
Enable Historical Requisitions View	When enabled, Historical Requisitions can be accessed in MyServices and Service Manager. Default is off.
Enable Historical Requisitions Scheduler	Requisitions that have been completed for more than 365 days are migrated to the historical transaction tables by default. The scheduler processes 1000 requisitions with a batch size of 100 for every 30 min of interval by default. These properties are configurable in the newscale.properties file and may be modified based on the specific needs of your organization. When enabled, Closed Requisitions will be archived. Default is off. For more information, see Run Processes, on page 241 and For details on directory integration, see the Cisco Prime Service Catalog Integration Guide.
Enable Service Catalog	When the setting is on, the module menu shows Service Catalog and Order Management instead of My Services. You may override this common setting by changing their profile preference. Default is on.
Enable Audit History	When enabled, Audit History will be tracked. Default is off.
Enable YUI	When the YUI setting is enabled, the YUI library is loaded in the Service Form. This ensures that the customizations that use the YUI, for example, the service wizard, works seamlessly. Disable the YUI setting if the YUI library need not be loaded in the Service Forms. Default is on.
Enable Go Button	When enabled, Go button will be available for active service, which is not orderable. Default is off.

Enable logs for Security Events	When enabled, log will be available for Security Events.
	Default is off.
Enable SAML	When enabled, you can configure SAML SSO login. If you enable SAML, LDAP SSO log in must be manually disabled.
	Default is off.

Style-Related Settings

Turning on custom style sheets and 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 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 Catalog with an enterprise LDAP directory, which provides personnel (person and organization) data for use in Service Catalog, 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, see the Cisco Prime Service Catalog Integration Guide

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 is loaded into the target environment via alternate methods, either through manual entry using Lifecycle Center or by importing the standards data.

For more information, see the Cisco Prime Service Catalog Designer Guide .

My Services Settings

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

Table 81: My Services Settings

Field	Description
Show Plan In My Services	Allow customers to see the status of tasks in the delivery plan for their requested services.
	Default is off.

Field	Description
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 appear 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.
Show Rating and Reviews	This option shows or hides Rating and Reviews. When disabled, it prevents you from viewing all reviews and ratings that appears in : • The Service Catalog home page • The Browse Categories screen • The Services search menu • Open Orders • Completed Orders tab Default is on.
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.

Field	Description
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 Of feature for all users. **Note** This setting may be made obsolete in future versions. Additionally, Cisco strongly recommends granting Order on Behalf permissions 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.
Allow Bill To OU Selection	Allow My Services users to change the Bill To organizational unit in their service requests. Default is off.

Form Monitor

The Form Monitor appears to the right of a service form. It displays the dictionaries in the form. A dictionary is checked when all mandatory fields in that dictionary have been provided values. The mandatory field status check is not applied to grid dictionaries.

It may be confusing if a dictionary is hidden by a rule or ISF code after the service form appears; 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 appears 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 appears 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 appears 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 preconfigured. All, some or none can optionally appear on the left side of the My Services home page. If no My Services portlets appear, 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 want to further customize the use or appearance of portlets, you may do so using the Cisco Portal Designer, described in the Cisco Prime Service Catalog Designer Guide.

Service Manager Settings

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

Table 82: Service Manager Settings

Setting	Description
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.

Setting	Description
Effort Entry Is Mandatory	Providing an entry in the Effort field is mandatory for completion of a task. Default is off.
Enable Ad-Hoc Task Email	When enabled, Service Catalog 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 appear. Default is on.

Setting	Description
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 Refresh 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.
	Note From version 9.3.2 or later, if this option is enabled and when you click a requisition number from the Service Manager module, the corresponding task popup window opens. Either you click **Home** or you refresh from the main window the task popup window will close automatically. Default is off.

Service Link Settings

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 or to periodically purge messages for completed tasks. These options are explained in the Cisco Prime Service Catalog Designer Guide.

Table 83: Compress setting

Setting	Description
Compress Messages	Messages in the database are 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.

The following authentication settings control the authentication of inbound Service Link HTTP requests received through the HTTP/WS Adapter, Web Services Listener Adapter, or Service Item Listener Adapter:

Table 84: HTTP setting

Setting	Description
Inbound HTTP Request Authentication	When enabled, authentication is required for all Service Link inbound requests. Default is on.

Service Item

Service Item settings affect the appearance and behavior of the Service Item module.

Table 85: Service Item

Setting	Description
Service Item permissions refresh	Enabling this property will refresh user permissions on service items at user login. Default is off.

Tenant Management

Tenant Management settings affect the appearance and behavior of the Tenant Management .

Table 86: Tenant Management

Setting	Description
Show Organization Permission	Display or hide the **Organization > Permission tab**. Default is on.
Show Organization Roles	Display or hide the **Organization > Roles tab**. Default is on.
Show Functional Position	Display or hide the **Organization > Functional position tab**. Default is on.
Show User Extensions	Display or hide the **User > Extension tab**. Default is on.
Show User Permission	Display or hide the **User > Permission tab**. Default is on.

Setting	Description
Show All Roles	This will allow user to search all roles. If it is OFF, it will display only custom roles. Default is on.

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:

- 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.

Figure 14: Person popup

The definition of a Person Popup shown above results in a Person Search popup that looks like:

Figure 15: Search result

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.

Table 87: Entity Homes

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.

Setting	Description
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, see the *Cisco Prime Service Catalog Designer Guide* .

Application Locale

During localization if you add a new language in the Localization module, you will need to update the language to all existing and new users.

The settings in the Application Locale are used to configure the settings for creating new users. After the settings are configured and saved, users created will have the default settings. However, these settings can be overridden at the user creation time.

For more information about localizing the application, see 'Localizing Service Catalog Strings' chapter in Cisco Prime Service Catalog Designer Guide .

To enable a new language and the corresponding currency to all users:

Step 1   Choose **Administration** > **Settings** > **Application Locale**.

Step 2   Select the following fields appropriately:

- **Language**: Select the new language from the drop-down list.

  Note   The selected locale determines the default language of the new users only. Now you can optionally modify the locale of the existing users also, by setting the `admin.setlocale.global` property in the newscale.properties file to true.

- **Currency Locale**: Select the corresponding locale. For example, if the locale selected is German, the sample format displayed for the amount is specific to German.

- **Currency Symbol for Money**: The Currency Symbol for Money field controls if the currency symbol is displayed for the amount or not.

Step 3   Click **Update**.

Password Policies

An application needs to have strong passwords to avoid malicious attempts. Strong passwords protect the application and data from various threats and vulnerabilities. You enforce password policies on your application to encourage users to employ strong passwords and change them often.

You either integrate your application with LDAP or with the local database for user management and authentication. LDAP user passwords are part of an external system and are administered or governed separately i.e outside Prime Service Catalog. Therefore, when LDAP users login via Single Sign-on and/or External User Authentication these password policies are not enforced.

If you have used the local application authentication for user management, you must configure password polices in the Prime Service Catalog administration module to make your application more secure for the end users to access. The application applies password policies when you change passwords and displays error messages when there is policy violation.

Password policies are enabled by default. You can modify or disable any policy based on your requirement. Any changes to the password policies are applicable to the users during the next login validation.

If the user violates any password policy mentioned in the Table 88: Password Policies Configuration Table, on page 228, the user account is locked and the user must contact system administrator to reset the password. For more information about password reset, see Configuring People, on page 160.

To configure or update password policies:

Step 1   Choose **Administration** > **Settings** > **Password Policies**.

Step 2   Update policies as per Table 88: Password Policies Configuration Table, on page 228.

Step 3   Click **Submit**.

Note   Click **Reset** to revert the password policy configuration to default values.

Table 88: Password Policies Configuration Table

Policy	Description	Configuration Default Values and Example
Length Policy	This policy determines the minimum and maximum number of characters allowed in the password.	Default Values: • **Minimum Required Length** is 4 • **Maximum Allowed Length** is 127. The number of characters allowed ranges between 4 through 127. This is applicable to: • The Change Password link when you log on to Prime Service Catalog. • The Password field available in **Organization Designer > People > General**.

Policy	Description	Configuration Default Values and Example
Password Expiration Policy	This policy determines how long users can use a password before they have to change it. The aim is to force users to change their passwords periodically. Generally, you use a shorter period when security is very important and a longer period when security is less important.	Default Values: • **Password Lifetime**: 365 days • **Warning Period Before Expiry**: 14 days • **Grace Period**: 3 days • **Permanently Lockout on Expiry**: Enable the check box if you want the user account to be locked permanently. The user must contact the administrator to reset the password. An administrator can reset the password after deselecting the **IsLocked** field, as explained in the Table 57: General fields, on page 161. For example: • **Password Lifetime**: 10 days • **Warning Period Before Expiry**: 3 days • **Grace Period**: 2 days Consider a user updates his password on April 20 th . • The password expires on April 30 th . • The user gets a warning message on April 27 th . • User account is active until May 2 nd and is locked starting May3 rd, until user resets his password. This is applicable to: • HTTPS/WS inbound adapter • SIM task inbound • Task Service SOAP/RAPI • For user login through User Interface, NSAPI, and RAPI.

Policy	Description	Configuration Default Values and Example
Retry Policy	• This policy determines the number of times a user can attempt to login to the application with an invalid password before the user account gets locked out. • You can also configure the number of times the user account must be locked before the user resets his password. The user cannot reset password during the locked period and must contact system administrator to unlock the password. For more information about resetting a user's password, see LoggedIn User Password field in General Person Information, on page 161.	The default values are: • **Lockout Period**: 15 minutes. To configure other Lockout Period values, choose values from the drop-down list. If you choose **Permanent Lockout** Enable the check box if you want the user account to be locked permanently. The user must contact the administrator to reset the password. An administrator can reset the password after deselecting the **IsLocked** field, as explained in the Table 57: General fields, on page 161. • **Unsuccessful Attempts**: 5 For example, the user account is locked during the 4th unsuccessful attempt and the user cannot access the application for 15 minutes. This is applicable to: • HTTPS/WS inbound adapter • SIM task inbound • Task Service SOAP/RAPI • User login through User Interface, NSAPI, and RAPI.

Policy	Description	Configuration Default Values and Example
Password Measure Policy	Defines the strength of the password. During password reset, the application determines the strength of the password and displays an error message if it does not meet the minimum strength criteria. Password Measure Policy is derived from "NIST SP 800-63" standards and also uses regular expressions. **Note** The entropy for dictionary check in NIST SP800-63 is not considered. The application starts evaluating the password from character position mentioned in First Position to the character position mentioned in Last Position, based on regular Expression mentioned in regex. A password score is derived from the total score value and if it is greater than or equal to Minimum Password Strength the application accepts the password.	

Policy	Description	Configuration Default Values and Example
		The default values are mentioned in Table 89: Default Configuration Table for Password Measure Policy, on page 233.
		First Position: Enter the first position to be evaluated.The application starts evaluating from the nth character mentioned in the First Position, where n is an integer that defines the character position of the password.
		Last Position: Enter the last position to be considered during evaluation.The application stops evaluating at the xth character mentioned in last position, where x is an integer that defines the character position of the password.
		Regex: Enter a regular expression that the application must evaluate.
		Score: Define a score for the password. The application applies the score if the regex evaluates to true for characters from the first position to the last position.
		Score Type: Select if the score type has to be: • **Per Character**: The score is multiplied for the number of characters from first position to last position. • **Fixed Length**: The score is as defined for the characters considered for evaluation.
		Minimum Password Strength Recommended: Enter the score value. The password must be greater than or equal to the total score value to be accepted. Default value is 12.
		Description: The values that you enter in the Configuration table is rephrased so the user can comprehend.
		Click **Add** to add more rows to configure the password measure

Policy	Description	Configuration Default Values and Example
		policy. This is applicable to change password and person update done through Organization Designer, import event in directory integration, and through directory task available in delivery plan.

Table 89: Default Configuration Table for Password Measure Policy

Row Number	First Position	Last Position	Regex	Score	Score Type
1	1	1	.	4	Per Character
2	2	8	.	2	Per Character
3	9	20	.	1.5	Per Character
4	21	End of String	.	1	Fixed Length
5	1	End of String	[^a-z]+	6	Fixed Length

Example for Password Measure Policy

Consider a password as Catalog@2014. Table 90: Example for Password Measure Policy, on page 233 table explains how the password measure policy is calculated based on configuration mentioned in Table 89: Default Configuration Table for Password Measure Policy, on page 233.

Table 90: Example for Password Measure Policy

Row Number	First and Last Character Position	Characters	Score per Character Type	Total Score
1	1 to 1	C	4 per character	4
2	2 to 8	atalog@	2 per character	14
3	9 to 20	2014	1.5 per character	6

Row Number	First and Last Character Position	Characters	Score per Character Type	Total Score
4	21 to End of String	not considered because the password does not have more than 20 characters.	1	0
5	1 to End of String	Catalog@2014	6	6
Total Score = 30 is greater than 12 ie **Minimum Password Strength Recommended**				
Result Password Accepted				

Debugging Settings

The Debugging settings 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).

Figure 16: Debugging page

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.

Table 91: Debug Settings

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.

Setting	Description
Directory Map Testing	Enables testing of a mapping used by directory integration. For more information see the Cisco Prime Service Catalog 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 Catalog encounters an error in processing a requisition submission or task authorization request asynchronously, the failed messages appear 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**.

Data Source Registry

The Service Catalog uses data sources defined in the data source registry to access application and to access user data stored in relational databases. By default, Service Catalog 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 data source, see the Cisco Prime Service Catalog Installation and Upgrade Guide .

Public and Private Keys

The Public Key is used to secure the sensitive field using the public key and this secure field will be decrypted by the external system by using the corresponding private key. Public keys are used to encrypt AMQP messages in Secure String Format. The default secure string format is Bytes. For information, see section Managing AMQP Connections, on page 245.

Table 92: Adding Public and Private Keys

Field	Description
Name	Enter the name of the recipient that must be included in the outbound message to achieve authentication and confidentiality.
Modulus	Enter the encrypted data.
Exponent	Enter a prime number that is not too large.
GUID	Based on the values specified for Name, Modulus and Exponent, the system generates a GUID that cannot be modified/edited. Globally Unique Identifier (GUID) also known as Universally Unique Identifier (UUID). This GUID is used for adding external layer of security for password and token.

Field	Description
Cipher Algorithm	Enter a Cipher Algorithm. It is an algorithm for performing encryption or decryption-a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code.
Impl Class Name	Enter a referred Class name to Key generation.

Support Utilities

Support Utilities includes the following:

- Logs and Properties, on page 236
- Purge Utilities, on page 239
- Version History, on page 240
- Form Data Viewer, on page 240
- Undelivered Email, on page 241
- Run Processes, on page 241
- Enabling Service Design Change History, on page 242

Note In order to see and use Support Utilities, the **Use Support Utilities** capability must be enabled for the user (see the Capabilities for Administration, on page 186).

Logs and Properties

If not already chosen, click **Logs and Properties** to view the Logs and Properties page.

Note In order to see and use Logs and Properties, both the **Use Support Utilities** and **Access Logs and Property Files** capabilities must be enabled for the user (see the Capabilities for Administration, on page 186).

Log and Destination Folder Settings

To use Logs and Properties, 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 delete them. You can create and specify a different destination folder for each file type.

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 or folders location and maximum size are specified in a support.properties file. There are two **support.properties** files—one for Service Catalog and one for Service Link.
These support.properties files are located in the following deployed directories:

- Service Catalog: RequestCenter.war/WEB-INF/classes/config/

- Service Link: ISEE.war/WEB-INF/classes/config

Note The paths above are for a Linux environment.
Open the support.properties file in a text editor.

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

Note For the Service Catalog support.properties file, only the Service Catalog entries are used; the Service Link entries are ignored. For the Service Link support.properties file, only the Service Link entries are used; the Service Catalog entries are ignored. The destination folder should be kept outside the application install directory to avoid crashing of the application in case a large file is compressed.

Figure 17: Support Properties


```
support.properties - Notepad

File  Edit  Format  View  Help

####################### NOTES #######################
##
##   Enter full directory path for each "*.destinationFolder.location" parameter.
##       For Windows: Use double-back-slash as directory separator; for example, C:\\CiscoServicePortal\\RC_log_dest.
##       For UNIX/Linux: Use single-forward-slash as directory separator; for example, /opt/CiscoServicePortal/RC_log_des
##   Enter a numeric value for each "*.destinationFolder.size.limit" parameter.
##       The unit of measure is GB.
##       Decimal number is acceptable.
##   For WebSphere or WebLogic, enter the full path for the application server's log directory in the "*.log.location" pa
##   For JBoss, the "*.log.location" parameter should be left blank.
##
####################################################

########  Request Center - Log Files
requestcenter.log.destinationFolder.location=C:\\CiscoServicePortal\\RC_log_dest
requestcenter.log.destinationFolder.size.limit=1
requestcenter.log.location=

########  Request Center - Property Files
requestcenter.property.destinationFolder.location=
requestcenter.property.destinationFolder.size.limit=1

########  Service Link - Log Files
servicelink.log.destinationFolder.location=
servicelink.log.destinationFolder.size.limit=1
servicelink.log.location=

########  Service Link - Property Files
servicelink.property.destinationFolder.location=
servicelink.property.destinationFolder.size.limit=1
```

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

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

Step 4   For 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 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 appears.
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 Catalog server.

View and Download Files

To view and download files:

Step 1   On the Logs and Properties page, choose a file type from the drop-down menu on the top left.
Four types of files can be chosen:

- Service Catalog – Log Files

- Service Link – Log Files

- Service Catalog – Property Files

- Service Link – Property Files

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

Step 3   To view a file, choose the number of last lines to view by choosing the number from the drop-down menu on the bottom
of the top pane, and then click **View**.
The file opens in a popup window.

Step 4   Click **Close** to close the window.

Step 5   To download one or more chosen files (**Ctrl-Click** to choose multiple files) to a location of your choice, click **Compress**.

Step 6   On the bottom pane, click **Refresh** to see the compressed file or files in the bottom pane. The file is compressed into the
Zip format and a time stamp is added to the name. For multiple files, a single Zip file is created (named only from the
file type and time stamp) containing all the chosen files.
  Note If the same file is compressed again, a new file with a different time stamp is created—the previously compressed
      file is not overwritten.

Step 7   On the bottom pane, click the Download icon for a single file.
A File Download dialog box appears. Click **Save**.

Step 8 A Save As dialog box appears allowing you to save the file to a location of your choice.

Step 9 Navigate to the location you want and click **Save**.

Step 10 After saving the file or files, you can delete the chosen compressed file or files (**Ctrl-Click** to choose multiple files) from the bottom pane by clicking **Delete**.

Purge Utilities

Choose **Administration** > **Utilities** > **Purge Utilities to view the Purge Utilities page**.

> **Note** In order to see and use Purge Utilities, both the **Use Support Utilities** and **Access Purge Utilities** capabilities must be enabled for the user (see the Capabilities for Administration, on page 186).

The three types of purge utilities are described below:

- **Requisition –** The requisition purge utility deletes requisitions 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 requisition purge utility 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 requisition purge utility is not optimized for mass data deletion and should be used with caution to avoid impacting the system response times for other application users.

The requisition purge utility 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.

- **Service Link –** The Service Link 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.

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

The Business Engine purge utility may require an hour or more to execute if you have a large database. Hence the purge should be done during a low activity time window. A practice run is recommended on a sandbox environment to establish how long the utility will run for your database.

To perform a purge:

Step 1   Click the radio button next to **Requisition, Service Link**, or **Business Engine** to choose the type of purge.

Step 2   Enter date ranges to filter the data to be purged. For a Requisition purge, you may also optionally filter the data by Requisition ID, Requisition Status, and Service Name.

Step 3   (Optional) Before performing a Requisition purge, click **Analyze** to perform a "dry run" purge. Click OK to continue. This allows you to see the requisitions that would be removed without actually deleting anything. This can serve as a validation for the filter criteria in effect. Go to Step 7.

Step 4   Click **Purge** to start the purge.

Step 5   Click Yes to continue.

Step 6   The purge starts. Click **OK**.

Step 7   Click Refresh after some time. When the purge or analysis completes, a new date/time entry is added in the Purge History pane at the top of the list. You must refresh the screen to see the new purge completion date/time entry.

Step 8   In the Purge History pane, click the purge completion date/time entry to see purge or analysis information in the Log Content pane on the right.

Step 9   If you did a Requisition purge analysis (Step 3), go to Step 4 above to start the actual purge.

Performance Considerations for Executing Purge

Purging can be performed while the Service Catalog application is up and running. However, you should limit the amount of purge activities during peak hours, and instead plan on doing large volume purging during off hours.

The purge utilities are also available as SQL scripts or batch programs that can be scheduled for execution. See the Optimizing Performance through Purging and Partitioning, on page 14 for more information.

Version History

Click **Administration > Utilities > Version History** to view the Version History page.

> **Note**   In order to see and use Version History, both the **Use Support Utilities** and **Access Version History** capabilities must be enabled for the user (see the Capabilities for Administration, on page 186).

The Version History page displays the current product version number of Service Catalog and a version history of build upgrades and patches.

Form Data Viewer

Click **Administration > Utilities > Form Data Viewer** to view the Form Data Viewer page.

> **Note**   In order to see and use Form Data Viewer, both the **Use Support Utilities** and **Access Form Data Viewer** capabilities must be enabled for the user (see the Capabilities for Administration, on page 186).

The Form Data Viewer, used primarily by service designers to verify the design of a service, allows you to see what values are actually stored for service forms in saved or submitted requisitions. It is useful when form rules associated with a service form are taking effect during form load. In this case, what is shown in the user interface does not really reflect what has been stored.

Enter a Requisition Entry number and click **Retrieve** to see the stored values in the table below. Click **Export to Excel** to export the values to an Excel spreadsheet for further analysis.

The Requisition Entry number can be located in the browser URL while you are on the Edit Service or Service Status page in My Services. It is shown as "reqentryid".

Undelivered Email

Undelivered Email utility provides a list of authorization, review, or notification emails that were undelivered to the recipient. You can view, resend, or delete the undelivered emails appropriately.

To resend undelivered emails:

Step 1	Select **Administration** > **Utilities** > **UnDelivered Email**.
Step 2	Click the Requisition ID or use the Search tab to search for the requisition.
Step 3	Review the email in the Message window
Step 4	Click **Resend**.

Run Processes

You can use this utility to migrate historical requisitions to the historical data tables on an adhoc basis. The manual migration process in an off-peak period will reduce the system overhead.

The values that are configured in newscale.properties file are displayed in the cut-off date, batch size, and maximum number of requisitions fields accordingly. You can further edit the settings and then click **Start** to enable the scheduler.

The processing rate and duration vary based on the average size of the requisitions. Work with your database administrator to perform trial runs and estimate the time required for the first-time execution, before executing the migration process in your production environment. For more information, see Optimizing Performance through Purging and Partitioning, on page 14.

To start the migration process:

Step 1	Select **Administration** > **Utilities** > **Run Processes**.
Step 2	Select a cut-off date using the calendar.
Step 3	You can also choose to enter a batch size and the maximum number of requisitions that you can process.
Step 4	Click **Start** to begin the migration process. Ensure that the Enable Historical Requisitions Scheduler setting in **Administration > Settings** tab is turned off. You can choose to process historical migration either by enabling the historical scheduler in or by using the Run Process Utility.

Stopping the Migration Process

Step 1   Select **Administration** > **Utilities** > **Run Processes**.

Step 2   Click **Stop** to terminate migration process that was enabled using the scheduler or the utilities.

Enabling Service Design Change History

When multiple users create service in active forms, it is difficult to know the changes what each user has done. Prime Service Catalog helps you to track these changes in service design using the Service Design Change History option. This will help to make the change details available for user access in Service Designer. For more information on how to track service design change history, see Cisco Prime Service 11.0 Catalog Designer Guide.

Audit History can be enabled by selecting "Enable Audit History" option in the Common settings. If Audit History is disabled then no new audit history entries will be stored, but the older data will be retained if the data falls within the retention period specified. When upgrading from an older version to a new version the audit history data will not be lost during upgrade.

What to Do Next

- Set the audit history retention period in **Administration > Customization**. Based on the retention period set here, system will check for the records and will delete the records older than the specified duration from the audit history tables. For more information on the retention period field and the minimum and maximum days that can be set for the audit retention period, see Customizations.

- By default, the scheduler processes the older data once in every week. To modify the duration of the scheduler, edit the audit poller in newscale.properties file.

SAML Configurations

The Security Assertion Markup Language (SAML) is an XML based open standard data format for exchanging authentication and authorization across domain and product. SAML 2.0 protocol offers SSO across Prime Service Catalog and CloudCenter, and enables federation between Prime Service Catalog and an Identity provider (IDP).

Note   The Prime Service Catalog 12.0 release supports only one IDP connection to authenticate a user at login.

The SAML Configurations includes the following:

- SAML Configuration
- Configuring IDP Mappings

- Refresh MetaData

For detailed information on SAML Configurations, see the Configuring SSO Using SAML chapter of Cisco Prime Service Catalog Administration and Operations Guide.

SAML Configuration

This section provides information on how to configure the SAML configuration in the Prime Service Catalog:

Before You Begin

Ensure to configure your IDP. Instructions to configure your chosen IDP is not in the scope of this document. Refer to the respective documentation for instructions.

Step 1   Choose **Administration > SAML SSO Settings**.

Step 2   Click **SAML Configuration** to configure SAML.

Step 3   Enter the following mandatory information in the **Configuration Information** page:

- EntityID—Enter Entity identity to identify the SAML configuration.

- Certificate(B64Encoded)—Paste the certificate contents here.

- Private Key(B64Encoded)—Enter the private key details here.

These field are automatically populated with the Prime Service Catalog certificate and private key once the server boots up. However, you could use a CA or Self-Signed certificates generated from the Open-SSL or Java Key tool. Certificates should be in Bas-64 encoded format.

Step 4   Click **Update**.
Note   You must restart the server for the changes to take effect. In a cluster set up, you must restart every individual nodes for the settings to take effect.

Step 5   Click **Download MetaData** to download the metadata.
Download metadata is an XML file that contains the SP entity ID and certificate. This metadata is used to register into the respective IDP so that IDP can identity the SP when the request comes from SP.

Configuring IDP Mappings

This section provides information on how to configure the SAML mappings in the Prime Service Catalog:

Before You Begin

Download the IDP metadata from the IDP you prefer to use and keep it handy. For example, for ADFS, you can download the metadata from the URL:
https://<server_domain_Name>/FederationMetadata/2007-06/FederationMetadata.xml

Step 1   Choose **Administration > SAML SSO Settings**.

Step 2   Click **IDP Mappings** to add a mapping in SAML Dashboard.

Step 3   Enter the following information in the **Mapping Information** page:

- Name—Enter unique name to identify the IDP configuration. This name cannot be edited once you save the mapping.

- MetaData—Paste the MetaData contents of IDP that is downloaded from the IDP.

Step 4   Enter the **Mapping Information**. The mappings prefixed with an asterisk (*), shown in the Mapping Information section, are mandatory.

- The attributes on the left hand side are person profile irrespective of the users roles or capabilities. Any user on successful login would use the right hand side attributes from IDP to match it to Left hand side attributes of Prime Service Catalog.

- The SAML assertion attributes on the right hand side is passed from IDP to SP (Service Catalog) on successful authentication.

Step 5   Click **Save**.

✎

Note
- You must restart the server for the changes to take effect. In a cluster set up, you must restart every individual nodes for the settings to take effect.

- Once you enable SAML, you can access the Prime Service Catalog only from the IDP login page.

- If you want to do housekeeping activities after configuring the SAML SSO then you must access the Prime Service catalog from backdoor URL
http://<ipaddress>:<port>/RequestCenter?Astalavista=true.

Refresh MetaData

You can click **Refresh Metadata**, to refresh the node on cluster before it kicks off the scheduled refresh activity every 24 hours.

Manage Connections

Manage connections allow you to create multiple Web Services and AMQP connections. The subsequent sections contain details on how to create and manage these connections.

Managing AMQP Connections

The AMQP username and password along with other AMQP settings can be used to establish connection with the RabbitMQ server. From this release onwards, multiple AMQP Connections are supported. The AMQP Public Key is used to secure the sensitive field using the public key and this secure field will be decrypted by the external system by using the corresponding private key. The AMQP Secure String Format is the format in which the data is encrypted. The default secure string format is Bytes. For information on configuring AMQP tasks for publishing service request to an external system, see Cisco Prime Service Catalog Designer Guide.

Connecting to RabbitMQ Server

You can establish communication with the RabbitMQ server by providing the AMQP credentials, under **Administration** > **Manage Connections** > **AMQP**. After you provide the details ensure to save your setting and click **Test AMQP Connection** to validate.

When you click **Test AMQP Connection**, the AMQP connection information is directly inserted into the database without going through the UI. The connection is saved only if AMQP connection authentication is successful. For more details, refer to **REST-based nsAPIs** section of the **Integrating with AMQP** chapter in *Cisco Prime Service Catalog Integration Guide*.

Table 93: AMQP Settings

Field	Description
Identifier	Enter a unique identifier for the connection.
Name	Enter a name for the connection.
Host Name or IP Address	Enter the IP address or the host name of the server where RabbitMQ is installed. If you are using cluster, enter the IP address or the host name of the server where RabbitMQ HA proxy is installed.
Protocol	Select the supported protocol from the drop-down, TCP or SSL.
Port	Displays the port number for RabbitMQ to connect with Prime Service Catalog. This field is auto populated based on the port number you select in **AMQP Port Type**. Default is 5672. **Note** If the ports configured are different than what is defaulted, Users can change it and click the 'Update' button to save the same.
Certificate	If you are using the protocol as SSL, then click on the **Certificate** option to add a valid SSL certificate. In case of AMQP cluster, if you select this option, you can connect to the HA proxy only if the user has a valid SSL certificate. **Note** If you do not click this option, then you will not be able to connect to SSL.
Skip Certificate Validation	Check this check box to skip the certificate validation .
User Name	Enter the username to connect to the RabbitMQ server.

Field	Description
Password	Enter the password to connect to the RabbitMQ server.
Virtual Host	Enter the virtual host to connect to the RabbitMQ Server, either locally or via remote client. Default corresponds to '/' in RabbitMQ server.
Public Key	The AMQP Public Key is used to secure the sensitive field using the public key and this secure field is decrypted by the external system by using the corresponding private key.
Secure String Format	The AMQP Secure String Format is the format in which the data is encrypted. The default secure string format is Bytes.
Server Down Notification	Select an e-mail template to notify one or more users if the AMQP cluster nodes goes down when a service request is ordered. The system will generate e-mail notifications for any of the following tasks: pre, post, or main tasks.
Recovery Interval	The AMQP recovery Interval is the interval between recovery attempts in minutes for AMQP Connection. Default value is 5 and value range is 1 to 60.
Inbound Queue	Enter the queue to which Service Catalog listens to for inbound messages. For inbound messages a dedicated queue *psc_inbound_queue* is created in RabbitMQ. This name can be modified if required.
Message Type	Select the message type format from the drop-down. This defines the default message processing format for all the outbound and inbound messages for the particular connection.

Note   Prime Service Catalog assumes that the RabbitMQ server is installed with a username and password.

- If SSL is supported, the required configuration changes must be done and the ports must be enabled on SSL. For more information on enabling SSL for RabbitMQ server, refer to RabbitMQ documentation.

- AMQP tasks, configured in the Service Definition, use the connection information provided in the Administration module for message publishing. In addition, this information is used by the Overview API to return RabbitMQ details to the caller.

- When the particular connection is saved successfully, a persistent AMQP connection from Prime Service Catalog to the AMQP Server is established to do the following:

  ◦ Republishing of outbound AMQP message when the AMQP server goes down and comes back again.

  ◦ Processing of inbound messages.

- The AMQP Public Key created in the **Administration** > **Settings** > **Public/Private Keys** will be available for selection for every new AMQP connection that is created.

Managing AMQP Tasks and Queue on RabbitMQ Server

Prime Service Catalog includes an administrative utility that allows you access the AMQP tasks queue on RabbitMQ Server instead of managing them on the RabbitMQ Server. You can access this console from **Administration > Utilities> AMQP Topics**. You can view all the available tasks for the chosen connection and delete any unwanted tasks. You can filter the available tasks for the selected connection based on one of the following criteria:

- All Exchanges: List all exchanges on RabbitMQ server

- In Used Exchanges: Exchanges for service requests that are in progress or are in active state and exchanges at service definition time.

- Orphan Exchanges. Exchanges that do not have references to any service definitions or are created by an external system.

Republishing AMQP Messages on RabbitMQ Server

Prime service Catalog offers an administrative utility that allows you to manually republish the AMQP messages to the RabbitMQ Server for the services that you have ordered.

Step 1 Go to **Administration** > **Utilities** > **AMQP Message Republish**.

Step 2 Enter the requisition id for the service for which you want to republish the message, and then click **Fetch Tasks**.

Step 3 Select the task and then click **Resend Message**.

Managing Webservices Connections

The Webservices allows you to access the services and functions defined by the Webservices. The Webservices tab in the Manage Connections page contains all information of the Webservices connection details that can be used in the Service Designer Active Form Components DDRs. The connection details are moved from the Dynamic Data Retrieval (DDR) to a centralized place, from which the details can be reused in the service designer. From 12.0 onwards, you can add multiple webservice connections. To add a webservice connection perform the following procedure and you will need to provide the connection details for the Webservice:

Step 1 Choose **Administration** > **Manage Connections** > **Webservices**.

Step 2 Click + **icon** and enter the following details to connect to the server.

Table 94: Integrating Webservices

Identifier	Enter a unique identifier for the webservice connection.
Name	Enter a name for the Service.
Host Name or IP Address	Enter a host name or the IP address of the server.

Protocol	Enter the required protocol, HTTP or HTTPS.
Port	Enter the port number of this Host name or IP address, default is 80 for http and 443 for https.
Certificate	Enter a valid certificate to connect to the server.
Skip Certificate Validation	Check this check-box to skip the certificate validation.
User Name	Enter the user name of the connection to the corresponding IP address or Host name.
Password	Enter the password of the Host name or IP address.
Authentication Mechanism	Select the required authentication, Session or Header.
Basic Authentication	Check this check box for basic authentication.
UserName Params	Enter the user name parameters, this entry is not mandatory.
Password Params	Enter the password parameters, this entry is not mandatory.
Login URL	Enter the URL to get the authentication/session token for API calls.
Authentication TokenParameter	Enter the authentication token parameter.

Step 3   Click **Save** and click **Test Connection** to authenticate the credentials.

Note

1   If the service with webservices DDR connection is exported and imported on different instances of Prime Service Catalog of same release, the Identifier and Name is displayed as the same name provided by you while creating the service.

2   If the service is imported from the previous release, the Identifier and Name for the webservice is created as I1, l2, and so on.

  Where, I indicates Import and the number changes incrementally as you import new services.

3   If the service with webservices DDR connection is upgraded by running the installer from the previous release, the Identifier and Name is created as W1, W2, and so on.

  Where, W indicates Upgrade and the number changes incrementally as we upgrade new services.

Note   For more information on how to export and import of a service, see *Exporting and Importing a Service* in Cisco Prime Service Catalog 12.0 Designer Guide.

APPENDIX C

Custom Themes

This chapter contains the following topics:

Custom Themes

Overview

This chapter describes the capabilities provided to customize the Service Catalog web pages. The customer-facing modules in the application can be customized using Cascading Style Sheets (CSS) and custom headers and footers.

The pages which may be customized include:

- Pages displayed in the Cisco Prime Service Catalog, My Services, and Service Manager modules including service forms dynamically generated, based on definitions specified via Service Designer

- The portals for Reporting and Advanced Reporting

- The login pages

- Preconfigured and custom portal pages in the Service Portal solution

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

Custom Style Sheets

Contents of the Service Catalog application are presented as web pages formatted using HTML5. Cascading Style Sheets (CSS) offer the ability to customize the web pages by changing the definition of themes used to display the pages, rather than having to edit the pages themselves.

Custom themes allow designers to customize Service Catalog web pages, headers and footer. Custom themes may be applied to all users of an application instance, or different themes 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 styles used in the built-in modules, namely My Services, Service Catalog, Service 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. In a Linux deployment this directory would be, /opt/CiscoPrimeServiceCatalog/jboss-as-7.1.1.Final/ServiceCatalogServer/deployments/RequestCenter.war/custom. The directory will typically have an images subdirectory, for any custom images. The directory name should indicate the tenant/organization name to which the style will apply.

2 If you use the Service Catalog module as the end user module, copy all the files located in the custom/ServiceCatalogExamples directory into the new directory created in Step 1. In a Linux deployment this directory would be, /opt/CiscoPrimeServiceCatalog/jboss-as-7.1.1.Final/ServiceCatalogServer/deployments/RequestCenter.war/custom/SmallCompany. If you use My Services module, copy all the files located in the custom/CustomExamples instead. Location of this archive will vary, based on your application server and installation setting.

3 In the new directory, remove the "example_" prefix of files in the directory as well as in the application directory under it. Modify the css files and add image files as needed to tailor the look and feel of the user interface as needed.

4 Use the Custom Styles page in the Administration module to define the style, specify the directory on which required files reside, and assign the organizations to which the style name applies.

5 Use the Settings page in the Administration module to turn on custom stylesheets.

6 Restart the browser session of Service Catalog—the pages should appear with the customizations applicable to the logged in user. You must exit and restart the Service Catalog 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 Catalog 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.

Defining a Custom Theme

A CSS Style designer will put the CSS in a directory on the server. In the example below you name a custom Style, and then associate it with a Style Directory, enter the description, and specify whether this style should apply to every user for the site, the sub-OUs under the associated Organizational Units, and whether it should apply to the Service Catalog module.

Fill in the properties as follows:

To start using custom style sheets or headers and footers:

Step 1   Log in to Service Catalog, choose the **Administration** module, and go to the **Settings** tab.
The Customizations page appears.

Step 2   At the right side of the screen, choose the **Custom Themes** option from the option list.

Step 3   Click **Add** to create a new theme.
The Custom Theme Properties page appears. See the below table to understand the Custom Theme Properties.

Step 4   Fill in the properties and click **Create** to create the theme. You can then edit the theme, to specify the organizations to which the theme applies.

Step 5   Click **Add** in the Associated Organizational Units pane. The Organizational Unit Search window appears. Choose one or more organizational units.
Note   You must create an user (see Adding a Person section) and add that user to the organizational unit. Only the user who is a member of the organizational unit can view the customization.

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

Table 95: Custom Theme Properties

Field	Description
Name	The theme name should reflect the OU or group of OUs the organizations to which the styles will apply.
Description	(Optional) Provide a description for the custom theme.
Apply this Theme to all subOUs	If a hierarchical structure is used in the organizations, you may specify that a theme is inherited by all child OUs of a parent.

Field	Description
Classic Custom	You may choose the Theme Directory from any directory under RequestCenter.war\custom. The directory must exist before you can create the theme. The default, a directory named 1, already exists.
Make this Theme the default for the entire site	One theme may be designated as the default. If a default is specified, it is used for any user whose home organization (OU) has not been assigned a theme. If no default is specified, the system-defined style sheets is used.
Apply the Theme to Service Catalog	You can also apply the CSS to Service Catalog module.
Website for Service Catalog	You may choose the Theme Directory from any directory under RequestCenter.war\Website. The directory must exist before you can create the theme. The default, a directory named ServiceCatalogWebsiteExample, already exists.
Website for Tenant Management	You may choose the Theme Directory from any directory under RequestCenter.war\Website. The directory must exist before you can create the theme. The default, a directory named TenantManagementWebsiteExample, already exists.
Website for Cloud Integrations	You may choose the Theme Directory from any directory under RequestCenter.war\Website. The directory must exist before you can create the theme. The default, a directory named CloudIntegrationsExample, already exists.

Customizing Service Catalog, Tenant Management, and Cloud Integrations Modules

Website model provides enhanced capabilities to customize certain modules of Prime Service Catalog such as, Service Catalog Tenant Management, and Cloud Integrations. You now have complete control to redesign the UI by applying customization (except for the Service Form), such as, adding another bootstrap file, and adding routing html and js files.

To customize website model, perform the following:

Before You Begin

1 Add all the customized files in a directory under *RequestCenter.war\Website*. By default, ServiceCatalogWebsiteExample, TenantManagementWebsiteExample, and CloudIntegrationsExample directory exists.

2 For Tenant Management and Service Catalog modules, website must have the *index.html* as the entry point. For Cloud Integrations the entry points are, *dashboard.html* and *admin.html*.

   Example: http://<ServerURL>/RequestCenter/website/ServiceCatalogWebsiteExample/index.html

3 In the routing html files,

- Use the following script to load all css dependancies by importing headcss.html into all routing html files:

```
<script type="text/javascript" src="common/js/vendor/jquery/1.9.1/jquery.min.js"
></script>
        <script>
            $(function(){ $("head").load("headcss.html") });
        </script>
```

- Use the following scripts to get the dependent details like localized strings and user dependent details.

  - For Service Catalog module use the script:
  ```
  <script type="text/javascript"
  src="/RequestCenter/servicecatalog/api/v11/strings.action"></script>
          <script type="text/javascript"
  src="/RequestCenter/servicecatalog/api/v11/uservars.action"></script>
  ```

  - For Tenant Management module use the script:
  ```
  <script type="text/javascript"
  src="/RequestCenter/tenantmanagement/api/v11/strings-tenant.action"></script>
          <script type="text/javascript"
  src="/RequestCenter/tenantmanagement/api/v11/uservars-tenant.action"></script>
  ```

  - For Cloud Integration module use the script:
  ```
  <script type="text/javascript"
  src="/RequestCenter/clouddashboard/api/v11/strings.action"></script>
    <script type="text/javascript"
  src="/RequestCenter/clouddashboard/api/v11/uservars.action"></script>
  ```

- Use the following script to load the requirejs:

```
<script type="text/javascript"
src="common/js/vendor/requirejs/2.1.6/require.js"></script>
```

4 Add or modify the vendor file details in *common-config.js* file.

Note You must place *js/configs/common-config.js* file on the website directory only.

Step 1 Log in to Service Catalog, choose the **Administration** module, and go to the **Settings** tab.
The Customizations page appears.

Step 2 At the right side of the screen, choose the **Custom Themes** option from the option list.

Step 3 Click **Add** to create a new theme.
The Custom Theme Properties page appears.

Step 4 Enter the **Name** and **Description** (optional).

Step 5 Check the **Website for Service Catalog** option to customize Service Catalog module, and browse to choose the Website Directory and click **OK**.
To customize website model for Tenant Management, check **Website for Tenant Management** and for Cloud Integration check **Website for Cloud Integration** option.

Remember If you uncheck the Website for Service Catalog checkbox, the Browse... option will be grayed out. When you check the Website for Service Catalog again, then the previously chosen website directory is selected by default.

Step 6   Click **Create** to create the theme. You can then edit the theme, to specify the organizations to which the theme applies.

Step 7   Click **Add** in the Associated Organizational Units pane. The Organizational Unit Search window appears. Choose one or more organizational units.

Step 8   You may edit the theme definition or the business units to which it applies at any time.

Enabling Custom Style Sheets and Headers/Footers

The appearance of customer-facing modules in the application can be customized using Cascading Style Sheets (CSS) and custom headers and footers.

Choose the Administration module, and go to the Settings tab. The Customizations page appears. The Common settings include parameters to "Enable Custom Header Footer" and "Enable Custom Style Sheets".

The custom Style sheets are enabled by default. You can change the corresponding parameter setting from "On" to "Off." Save your changes by updating the page. Any specified in the custom.css file (in place on the application server) will be in effect.

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. There is a directory under RequestCenter.war/custom named ServiceCatalogExamples which provides the base application CSS files that you can customize for your brand as well as the GUI design.

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, on page 214 to increment the browser cache version.

Customizing Styles for Service Catalog Module

Files in the custom\ServiceCatalogExamples directory are available if you want to do more extensive customization of the UI. There are three main files to start with:

- before.html – The content of this file is prepended to the <body> of the HTML document. You can use this file to override product strings before they are displayed. For example, the product name in the header uses string ID 15162, so you can make the product show "Small Company" by inserting this block into before.html:

```
<script>
serviceCatalogMessage.putString("15162", 'Small Company');
</script>
```

Use Firebug or other web developer tools to examine the HTML code of the Service Catalog module. You will see other strings that you can override.

• head.html – The content of this file is injected into the end of the (head) section of the HTML document. You can override the colors and styles specified by the various HTML classes and elements on the web page. For example, change the color settings for the Small Company "homeslider" to something different:

```
<style>
.homeslider .blocks.block1 {
background-color: #9E6F9A; /*#2B6F9A;*/
background-image: linear-gradient(to bottom, #985DC2, #B6115E); /*#258DC2, #04415E);*/
background-repeat: repeat-x;
}
.homeslider .blocks.block2 {
background-color: #9E6F9A; /*#2B6F9A;*/
background-image: linear-gradient(to bottom, #D486C0, #B43557); /*#6486C0, #213557);*/
background-repeat: repeat-x;
}
.homeslider .blocks.block3 {
background-color: #9E6F9A; /*#2B6F9A;*/
background-image: linear-gradient(to bottom, #EE86C0, #BE3157); /*#7B86C0, #2B3157);*/
background-repeat: repeat-x;
}
</style>
```

• after.html – The content in this file is appended at the end of the html (body).

Here is a quick example on how to change the default Cisco Logo to some other company logo in the head.html file, as it is a style override:

-
```
<style>
.navbar-inner {
background-color: transparent;
background-image: none;
filter: progid:DXImageTransform.Microsoft.gradient(enabled=false); /*disable gray header
 bar in IE*/
}
.navbar .nav {
color: #333;
text-shadow: none;
}
.navbar .nav ) li ) a {
color: #333;
text-shadow: none;
}
.psc-goto-cart {
color: #333 !important;
}
.psc-top-icon {
border:2px solid #333;
background-color: #333;
}
/* Change company logo */
.psc-header.navbar.brand {
background-image: url("/RequestCenter/custom/SmallCo/images/SmallCo_logo92x33.gif");
background-repeat: no-repeat;
background-position: 0 .514em;
background-size:75px auto;
padding-left: 3em!important;
padding-top: 0.25em!important;
padding-right: 5em!important;
font-size: 1.571em;
line-height: 2.28em;
color: #333; /* Small Company's website H1 color */
text-shadow: none;
}/* Change company logo */
</style>
<style>
/* The following block changes the colors "Home", "Browse Categories" and magnifying
glass
(search) box to orange(!), including the search box hover state */
.categories > .navbar li.menu.menu > a, .categories > .navbar li.menuHome.menu > a,
.categories > .navbar li.search.menu > a {
background: none repeat scroll 0 0 orange;
}
.categories > .navbar li.menu > a, .categories > .navbar li.menuHome > a, .categories
 > .navbar li.search > a {
background: none repeat scroll 0 0 orange;
}
.categories > .navbar li.menu, .categories > .navbar li.menuHome, .categories > .navbar
 li.search {
background: orange;
}
.categories > .navbar li.menu:hover, .categories > .navbar li.menuHome:hover, .categories
 > .navbar li.search:hover {
background-color: orange;
background-image: linear-gradient(to bottom, orange, orange);
background-repeat: repeat-x;
}
/* This changes the navbar background color to the right of the Home, Browse Categories
 and magnifying glass box.*/
.categories > .navbar {
background-color: rgba(255, 255, 102, 0.75); /* this sets the color and transparency
of the navbar*/
}
.page-heading { /* This overrides the default : background-image:*/
url("../../ngc/img/page_heading_bg.png");
in the "Categories" view, so the color behind the "Categories" text is light green rather
 than the blue from the png.
background-color: lightgreen;
background-image: none;
}
```

```
            </style>
```

Customizing User-Defined Portals

Just like Service Catalog, My Services and other built-in modules, the Service Portal 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 Designer modules.

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

The custom stylesheet for Service Portal module is located in the same custom/ServiceCatalogExamples or custom/CustomExamples directory as Service Catalog 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 Catalog 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 chapter.
3 Copy this file into the custom directory created for the tenant/organization (see Customizing Built-In Modules, on page 252, Step 1) along with any images used.

Example

The following example describes how to modify the logo (92X33 pixels), product name and background color in the portal header:

```
.reboot2 .xwtBackgroundSimplified {
background: transparent !important;
}
/*style to modify logo image*/
.reboot2 .applicationHeader17 .applicationLogoImage {
background: url("images/SmallCo_logo92x33.gif") no-repeat transparent !important;
/*background-repeat: no-repeat;
background-position: 0 .514em;
background-size:75px auto;
padding-left: 3em!important;
padding-right: 5em!important;*/
height: 33px !important;
width:92px !important;
/* Note: un-comment display property to hide the Product Logo if needed */
/*display:none !important;*/
}
/* This style is used to display or hide the Product Title in Portal modules
See Also: .applicationHeaderAppSubTitle, .applicationLogoImage, .applicationHeaderLogoText
 style - which will be the new style used to display branding logo
*/
.reboot2 .applicationHeader17 .applicationHeaderAppName {
visibility: hidden;
}
```

The following example describes how to modify the logo (135x70 pixels), product name and background color in the portal header:

```
.reboot2 .xwtBackgroundSimplified {
background: transparent !important;
}
.reboot2 .applicationHeader17 {
padding-left: 5px !important;
}
```

```
/*style to modify logo image*/
.reboot2 .applicationHeader17 .applicationLogoImage {
background: url("/RequestCenter/custom/style_dir/images/custom_logo.png") no-repeat scroll
 -2px -8px transparent !important;
background-size: auto auto !important;
height: 73px !important;
line-height: 70px !important;
top: 1px !important;
width: 130px !important;
}
/*This style will reduce the left, right and top padding for logo container*/
.reboot2 .applicationHeader17 .applicationHeaderLogo {
margin-left: 2px !important;
margin-right: 2px !important;
padding-top: 5px !important;
}
.reboot2 .applicationHeader17 .applicationHeaderAppSubTitle {
color: #202020;
cursor: default;
font-size: 17px !important;
font-weight: bold !important;
font-family: CiscoSans,Arial,"Helvetica Neue",Helvetica,sans-serif !important;
text-shadow: 0 0.071em 0 #585858 !important;
}
```

The following example describes how to modify the product name and customize the PortalFullpagePrimeUi.js file. On Linux you can locate the file from the path /opt/CiscoPrimeServiceCatalog/jboss-as-7.1.1.Final/ServiceCatalogServer/deployments/RequestCenter.war/ns360/js/PortalFullpagePrimeUi.js. You can search for the function name "getNavItems" and change the name from 'Service Catalog' to 'Cloud Manager':

```
if(defaultSelectedId != ""){ /*existing code*/
navItems.items.defaultSelected = defaultSelectedId;
} /*existing code*/
navItems.items.toolbar.push(getToolbar()); /*existing code*/
/*Overwrite the app header text with custom application name "Cloud Manager"
If text need to add for AppName div then from custom css file its "visibility"
attribute should be "block !important"*/
var appNameDiv = dojo.query('.applicationHeaderAppName')[0];
appNameDiv.style.display = "block !important";
appNameDiv.innerHTML = "Cloud Manager";
var appSubTitleDiv = dojo.query('.applicationHeaderAppSubTitle')[0];
appSubTitleDiv.style.display = "block !important";
appSubTitleDiv.innerHTML = "Cloud Manager";
return navItems; /*existing code*/
```

Customizing Styles for MyServices Module

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

Table 96: Custom styles

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 Catalog styles which may be replaced via custom style sheets
common_task_bg.gif	Background for the Common Tasks pane

custom (folder) Contents	Description
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 Catalog 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 Catalog settings to start with, with solid color replacing gradients
example_portal-custom-header.css	Sample file, mirrors default Portal Designer 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 templates for your custom.css and portal-custom-header.css) are formatted as a standard cascading style sheet file and includes comments to guide you in choosing styles to modify. These comments include brief descriptions of where and how a particular style is used; however, some experimentation is 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.

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 side of the header. 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 corner.

Navigation Bars

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 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 Catalog 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.

Figure 18: Buttons on Service Form

1	Primary buttons
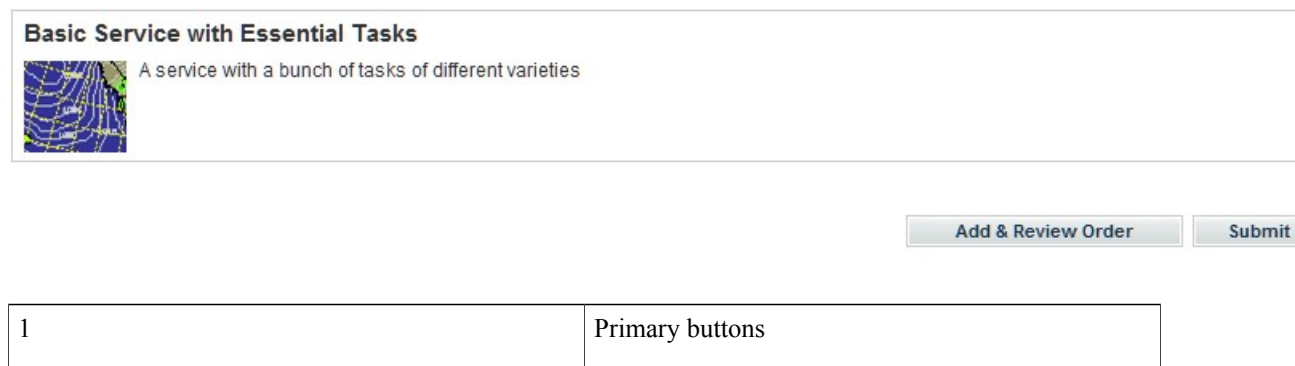
Service Forms

The appearance of the fields and captions 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.

Table 97: Service forms fields

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

Figure 19: Service forms

1	shortHeader
2	subhead

Note You can optionally enable the legacy display style for non-grid Dictionary field help texts by setting the `Serviceformelement.display.instructional.helptext` property in the newscale.properties file to true.

✎

Note   You can optionally enable the designers access to `Message_INFO ID` of Service Form input fields through java script, by setting the `serviceformelement.display.instructional.helptext.Message_INFO` property in newscale.properties file to true.

You must set the `Serviceformelement.display.instructional.helptext` property in the newscale.properties file to true to enable the access to `Message_INFO ID`.

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.

To preserve the customizations when you upgrade or migrate the application:

Step 1   Create an archive file in the Zip format containing the files you have customized. The archive directory structure must match the deployment directory structure. The root directory of the archive file should be the RequestCenter.war directory.

Step 2   Perform an upgrade of the Service Catalog application.
To avoid losing the customizations, the Service Catalog installation wizard allows you to specify custom content to be included in the installation:

Step 3   Run the Service Catalog installation wizard as described in the *Cisco Prime Service Catalog Installation Guide* , using the **Advanced Installation** type.

Step 4   On the Application Server Configuration page, click **Advanced Options**.

Step 5   The Advanced Options dialog box appears, as shown below.

Step 6   Check **Custom content**.

Step 7   Enter the full path to the **Custom content archive** including the name of the archive, or click **Browse** to locate and choose the custom content archive.

Step 8   Click **Close**.

Step 9   Continue with the installation as described in the *Cisco Prime Service Catalog Installation Guide* .

Step 10   While the Service Catalog installation wizard completes the installation, it extracts your custom content archive into the application deployment directory structure.

Known Errors and Omissions

The online help files provided for Service Catalog cannot be customized.

Unknown Errors and Omissions

It is possible that some styles used in Service Catalog 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 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 Catalog 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

This section describes the various style summary and the recommended practices.

Style Summary – Built-In Modules

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

Table 98: Available styles

Style/Class Name	Comment
Body and Global Styles	
body	
#lvl3_nav	
#headerlogo	Logo on the right
#leftheaderlogo	Logo on the left
#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	

Style/Class Name	Comment
.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

Style/Class Name	Comment
Header and Title Styles	
div.longHeaderdiv.shortHeader	
div.longHeader h4div.shortHeader h4div.longHeader spandiv.shortHeader span	
div.subHeader	
h4.header	
h4.header span	
Button Styles	
buttoninput.primaryinput.secondaryinput.disabled	
button.primaryinput.primary	
button.secondarybutton.helpinput.secondary	
button.disabledinput.disabled	
Catalog and Service Display Styles	
table.browser	
table.browser td.categoryImage	Pixel sizes for the Service Catalog and category images
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	

Style/Class Name	Comment
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 thbody.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:hovertable.fullGrid tbody.th.kvpKeyHi:hovertable.fullGrid tbody.td.kvpKeyHi:hover + td.kvpValuetable.fullGrid tbody.th.kvpKeyHi:hover + td.kvpValue	
table.fullGrid tbody.td.kvpKeyHitable.fullGrid tbody.th.kvpKeyHi	
table.fullGrid tbody td.kvpValueHi	
Other Tables and Table-Related Content Styles	

Style/Class Name	Comment
div.theaddiv tfoot	
div.tsubfoot	
div.detailHeader	
div.detailHeader td.owi	
div.tfoot input.textBoxdiv.tsubfoot input.textBox	
Comments and History Styles	
table.commentstable	
table.commentsTable div.commentContainer	
Common Tasks and Portlet Styles	
div.shell	
.commonTaskCellul.tasks.li	
ul.tasks	
img.commontaskbullet	
Normal Portlet, Form and Container Styles	
div.servicediv.shelldiv.smallshelldiv smallShelldivalGridabfdlGridabfooGridatashGridabmGridatexontanologinBox	
Input Elements	
inputselect	Service form text elements
input.textBoxtextarea	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

Style/Class Name	Comment
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	

Style/Class Name	Comment
Module Menus	
.modulemenu	
.modulemenu .menuheadingrow	
menuHighlight	

Style Summary – User-Defined Modules

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

Table 99: User defined styles

Style/Class Name	Comment
Header Styles	
#headerlogo	Logo on the right
#leftheaderlogo	Logo on the left
#lvl1_nav_title	Application name
#header	
#usercontrols	
#cornerpiece	
#moduleMenuDiv	
.modulemenu	
.menuHighlight	
#userinfoandcontrols	
#userinforow	
#usercontrolstable	
#userconrolsrow	
#profilef	
#logoutref	

Style/Class Name	Comment
#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 does not include all styles, it does cover the most commonly customized ones.

Figure 20: Sample Screen
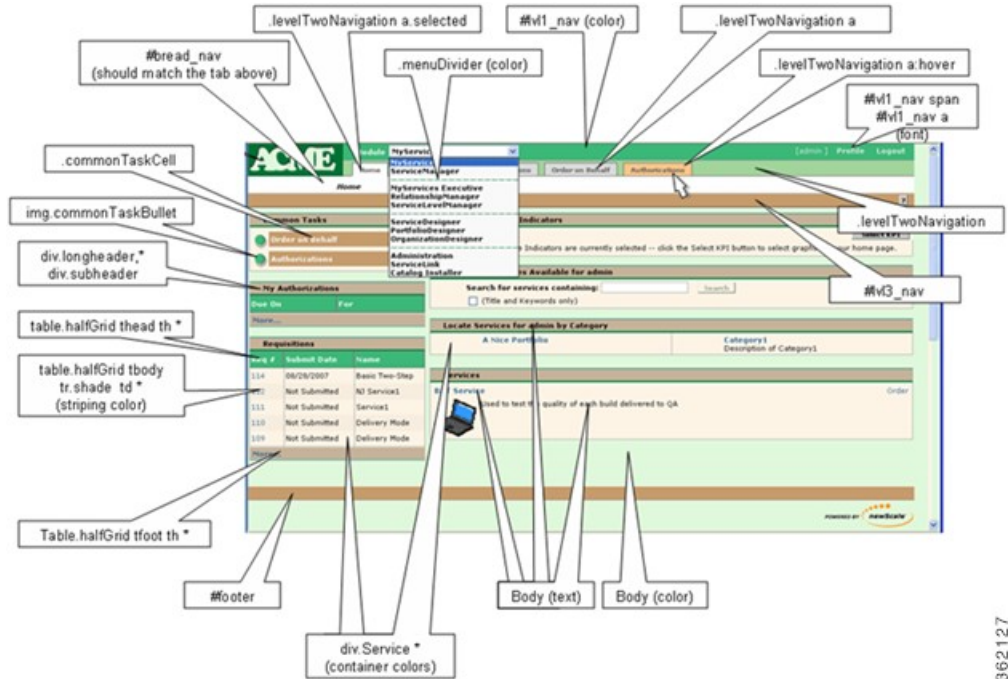
* Indicates that this is the first descriptor in the style grouping, and there are others.

Custom Headers and Footers

This section describes the updates to custom headers and footers.

Overview

Cisco supplies a template for customizing the page headers and footers that appear with Service Catalog web pages.

Procedure

Additional details on these styles are given in the section Customizing Page Headers and Footers, on page 274. To add a custom header or footer to the Service Catalog application:

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

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

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

Step 4 Place your custom header and footer files on the specified directory for the styles to which they apply. Both files must be present. If you are not using a custom header 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 Catalog—the pages should appear with your customizations.

Customizing Page Headers and Footers

Custom page headers and footers appear 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 Catalog 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.

Figure 21: Footer logo

I N D E X