



Configuring Site-Wide Settings

This chapter contains the following topics:

- [Configuring Site-Wide Settings, page 1](#)

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 1: 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 2.)
- 2 Specify the details for each type of authorization which has been enabled. (See [Specifying Authorization Details](#), on page 3.)
- 3 Optionally specify the escalation procedure to be followed if a required authorization is late. (See [Notifying Delayed Tasks](#), on page 6.)

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 2: 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*	<p>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.</p> <p>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.</p>
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	<p>Choose one of the following from the drop-down menu:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

Field	Description
Escalation Tiers	<p>Click one of the following:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
Evaluate condition when	<p>Choose either:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

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, #Performer.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](#).

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 1: Email Templates page

Email Templates

Request Center **Demand Center**

Name

- A01 - Service Complete2
- A02 - RACF Approval
- A03 - KP HealthConnect Form
- A04 - CPM Completed
- A05 - Onboarding Bundle Completion
- A06 - Bundle Submitted
- Ad-Hoc Task Started
- Approval/Review Failed
- Default late activity
- E1 - Approval Pending Notification

Items 1 - 10 of 40 Go

General

Name: A01 - Service Complete2 **Subject:**

From: internal@newscale.com **To(s):**

Type: ☒ Request Center ☐ Demand Center **Language:**

☒ HTML Part ☐ Text Part

Source **Format** **Font** **Size** **A** **A**

Requisition Number: #Requisition.RequisitionID#

Service Name: #Service.Name#

Requested For: #Service.Data.NEW_HIRE_INFO.Name#

Dear #Service.Data.RC_REQUESTEDFOR.FirstName# #Service.Data.RC_REQUESTEDFOR.LastName#

Your Request It Requisition # #Requisition.RequisitionID# for #Service.Name# has been completed.

Thank You,

Request It

NOTICE TO RECIPIENT: If you are not the intended recipient of this e-mail, you are prohibited from using, copying, distributing, or otherwise relying on the content of this e-mail. If you have received this e-mail in error, please notify the sender immediately by reply e-mail and delete this e-mail and any attachments. Do not forward or save them. Thank you.

Update **New** **Delete**

Configuring Templates

To configure an email template, supply the following information:

Table 3: 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 4: 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 10.

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](#)). 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 5: Site Settings page

Page	Description
Customizations, on page 11	Configure site-wide settings for various modules.
Person Popup, on page 24	Set the type of information that displays when conducting a person search.
Entity Homes, on page 25	Specify the definitional data that can be modified on the sites of an implementation.
Application Locale, on page 26	Ensure that all new users use the updated language and the corresponding currency.
Password Policies, on page 27	Define policies for configuring passwords.
Debugging Settings, on page 34	Specify whether to display debugging information within the user interface.
Data Source Registry, on page 35	View the data sources registered with the application.
Custom Themes	Define and specify the organizations to which they apply.
Public and Private Keys, on page 35	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 6: 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 <i>select (*)</i> 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 35 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 7: 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	<p>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.</p> <p>Default is on.</p>
Show Login Name	<p>Show or hide the display of person login name on the view person profile popup page.</p> <p>Default is off.</p>
Accept encrypted Password	<p>When enabled, the password used for inbound HTTP requests must be in encrypted format.</p> <p>Default is off.</p>
Enable Historical Requisitions View	<p>When enabled, Historical Requisitions can be accessed in MyServices and Service Manager.</p> <p>Default is off.</p>
Enable Historical Requisitions Scheduler	<p>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.</p> <p>When enabled, Closed Requisitions will be archived.</p> <p>Default is off.</p> <p>For more information, see Run Processes, on page 41 and For details on directory integration, see the Cisco Prime Service Catalog Integration Guide.</p>
Enable Service Catalog	<p>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.</p> <p>Default is on.</p>
Enable Audit History	<p>When enabled, Audit History will be tracked.</p> <p>Default is off.</p>
Enable YUI	<p>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.</p> <p>Default is on.</p>
Enable Go Button	<p>When enabled, Go button will be available for active service, which is not orderable.</p> <p>Default is off.</p>

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 8: 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 : <ul style="list-style-type: none"> • 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 9: 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	<p>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.</p> <p>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.</p> <p>Default is off.</p>

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 10: Compress setting

Setting	Description
Compress Messages	<p>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.</p> <p>Default is on.</p>

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 11: 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 12: 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 13: 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 2: Person popup

Person Popup	
Column Heading to Display	Request Center Person Data to Use for this Heading
Name	First Name Last Name
Organizational Unit	Home Organizational Unit

The definition of a Person Popup shown above results in a Person Search popup that looks like:

Figure 3: Search result

Select Person

* Search For:

Search Results

	Name	Organizational Unit
<input checked="" type="radio"/>	BAT Customer	B.A.T.Service Team
<input type="radio"/>	BAT DA	B.A.T.Service Team
<input type="radio"/>	BAT DR	B.A.T.Service Team
<input type="radio"/>	BAT FA	B.A.T.Service Team
<input type="radio"/>	BAT MANAGER	B.A.T.Service Team
<input type="radio"/>	BAT MANAGER2	B.A.T.Service Team
<input type="radio"/>	BAT SGA	B.A.T.Service Team
<input type="radio"/>	BAT SGR	B.A.T.Service Team

Items 1 - 8 of 8

Note: The number of people returned by open-ended search is currently limited by your Request Center administrator to 1,000.

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 14: 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 policies 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 15: Password Policies Configuration Table, on page 28](#), 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](#).

To configure or update password policies:

-
- Step 1** Choose **Administration > Settings > Password Policies**.
- Step 2** Update policies as per [Table 15: Password Policies Configuration Table, on page 28](#).
- Step 3** Click **Submit**.
- Note** Click **Reset** to revert the password policy configuration to default values.

Table 15: 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.	<p>Default Values:</p> <ul style="list-style-type: none"> • Minimum Required Length is 4 • Maximum Allowed Length is 127. <p>The number of characters allowed ranges between 4 through 127.</p> <p>This is applicable to:</p> <ul style="list-style-type: none"> • 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.	<p>Default Values:</p> <ul style="list-style-type: none"> • 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 1. <p>For example:</p> <ul style="list-style-type: none"> • Password Lifetime: 10 days • Warning Period Before Expiry: 3 days • Grace Period: 2 days <p>Consider a user updates his password on April 20th.</p> <ul style="list-style-type: none"> • The password expires on April 30th. • The user gets a warning message on April 27th. • User account is active until May 2nd and is locked starting May 3rd, until user resets his password. <p>This is applicable to:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. <p>For more information about resetting a user's password, see LoggedIn User Password field in General Person Information.</p>	<p>The default values are:</p> <ul style="list-style-type: none"> • Lockout Period: 15 minutes. <p>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 1.</p> <ul style="list-style-type: none"> • Unsuccessful Attempts: 5 <p>For example, the user account is locked during the 4th unsuccessful attempt and the user cannot access the application for 15 minutes.</p> <p>This is applicable to:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Password Measure Policy is derived from “NIST SP 800-63” standards and also uses regular expressions.</p> <p>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.</p>	

Policy	Description	Configuration Default Values and Example
		<p>The default values are mentioned in Table 16: Default Configuration Table for Password Measure Policy, on page 33.</p> <p>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.</p> <p>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.</p> <p>Regex: Enter a regular expression that the application must evaluate.</p> <p>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.</p> <p>Score Type: Select if the score type has to be:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Description: The values that you enter in the Configuration table is rephrased so the user can comprehend.</p> <p>Click Add to add more rows to configure the password measure</p>

Policy	Description	Configuration Default Values and Example
		<p>policy.</p> <p>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.</p>

Table 16: 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 17: Example for Password Measure Policy, on page 33](#) table explains how the password measure policy is calculated based on configuration mentioned in [Table 16: Default Configuration Table for Password Measure Policy, on page 33](#).

Table 17: 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 4: Debugging page

Debugging		
On	Off	Setting
<input checked="" type="radio"/>	<input type="radio"/>	Debug
<input checked="" type="radio"/>	<input type="radio"/>	Directory Map Testing

Update

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 18: 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 44.

Table 19: 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 36
- [Purge Utilities](#), on page 39
- [Version History](#), on page 40
- [Form Data Viewer](#), on page 40
- [Undelivered Email](#), on page 41
- [Run Processes](#), on page 41
- [Enabling Service Design Change History](#), on page 42



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](#)).

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](#)).

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:

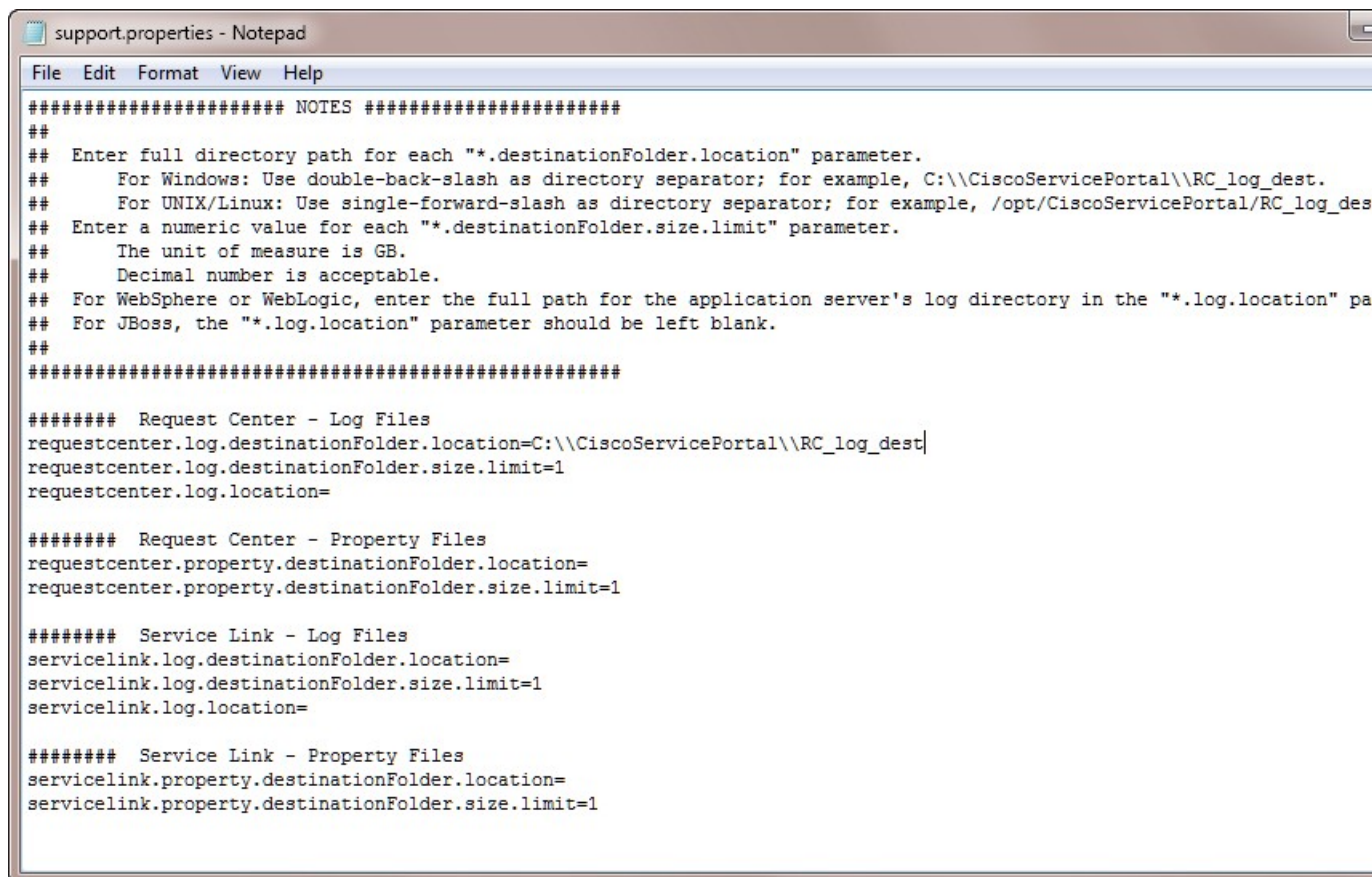
- Service Catalog: RequestCenter.war/WEB-INF/classes/config/
- Service Link: ISEE.war/WEB-INF/classes/config

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 5: 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_dest.
## 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" parameter.
## 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 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](#)).

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](#) 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](#)).

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](#)).

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](#).

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.

-
- 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:

-
- 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.

You must download the IDP metadata from the respective IDP. For example, for ADFS you can download the Metadata from the following URL: *https://<server_domain_Name>/FederationMetadata/2007-06/FederationMetadata.xml*.

Step 4 Configure the **Mapping Information** attributes based on the requirements documented in the Mapping Worksheet. 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 activates after configuring the SAML SSO then you must access the Prime Service catalog from backdoor URL.

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 20: 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.
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.

Field	Description
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 <i>psc_inbound_queue</i> 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 21: 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, I2, 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](#).