HP IT Operations Compliance

Software Version: 1.0

-

Administration Guide

Document Release Date: July 2015
Software Release Date: July 2015

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1 ITOC Administration **9**

View Administration in ITOC 9

Chapter 2 Users **11**

View Users in ITOC 11

Chapter 3 Roles and Permissions **13**

Roles 13

ITOC Roles and Responsibilities 13

Permissions 16

ITOC Permissions 16

Chapter 4 Notifications **20**

Notifications Overview 20

Subscribers 20

View Notifications 20

Edit Notifications 21

Configure SMTP for Notifications 22

Notification Types 22

Event-Driven Types 22

Business Service Revision Commented On 23

Business Service Revision Promoted to Production 23

Business Service Revision Promoted to Production, where Business Service is Associated with an SoA 23

Business Service was Obsoleted 23

Control Revision Commented On 23

Control Revision Promoted to Production 23

Control Revision Promoted to Production, where Control used in a Policy Rule 23

Control Revision Promoted to Production, where Control used in a Policy Rule, and Policy is associated with an SoA 23
Control was Obsoleted 24
Maintenance Window was Deleted and Auto-removed from SoA 24
Object Revision Approved 24
Object Revision Submitted for My Approval 24
Object Revision I Submitted was Rejected 24
Policy Revision Commented On 24
Policy Revision Promoted to Production 24
Policy Revision Promoted to Production, where Policy is Associated with an SoA 24
Policy Revision Promoted to Production, which Invalidated an SoA Exception 25
Policy was Obsoleted 25
Resource was Obsoleted 25
Statement of Applicability Revision Commented On 25
Statement of Applicability Revision Promoted to Production 25
Statement of Applicability Revision was Obsoleted 25
Reminder Types 25
Draft Revision In Draft State for N Days 26
Object Revision Has Been Awaiting My Approval 26
Object Revision I Submitted Has Not Been Approved 26
Policy Effective Date Is Coming Up Soon 26
Production SoA With Expired Exception(s) 26
SoA Revision Has Exception(s) Expiring Soon 26
Compliance Status 26
Business Service Meeting MSLO Changed 26
Business Service Meeting RSLO Changed 27
Overall Business Service Compliance Status Changed 27
Overall Policy Compliance Status Changed 27
Remediation Job Completed 27

Scan Job Completed 27
Chapter 5 Maintenance Windows 28
Maintenance Windows Overview 28
Maintenance Window Work Prioritization 28
View Maintenance Windows 29
Create a New Maintenance Window 29
Manage Maintenance Windows 32
Maintenance Windows Details 32
To edit maintenance windows properties... 33
To delete a maintenance window... 33
Maintenance Windows Jobs 34
Maintenance Windows Where Used 35
Chapter 6 Business Configuration 37
Compliance 39
Workflow 39
Business ID Prefix 39
Chapter 7 System Configuration 40
Chapter 8 Organizations 43
Organizations Overview 43
Public Provider Organizations 43
Consumer Organizations 44
Log Into the Organizations Administration UI 44
Create and Manage Organizations 44
Create a New Organization 45
Configure and Manage Authentication 48
Customize a Consumer Organization 51
Application Labeling 52
Add Groups and Associate Business Roles 53
Edit Groups 54

Delete Associated Roles 54
Remove Groups 54
Disable Seeded Users 54
Business Roles 56
Delete an Organization 56

Chapter 1 ITOC Administration

This guide provides instructions and reference for ITOC administrator tasks, such as:

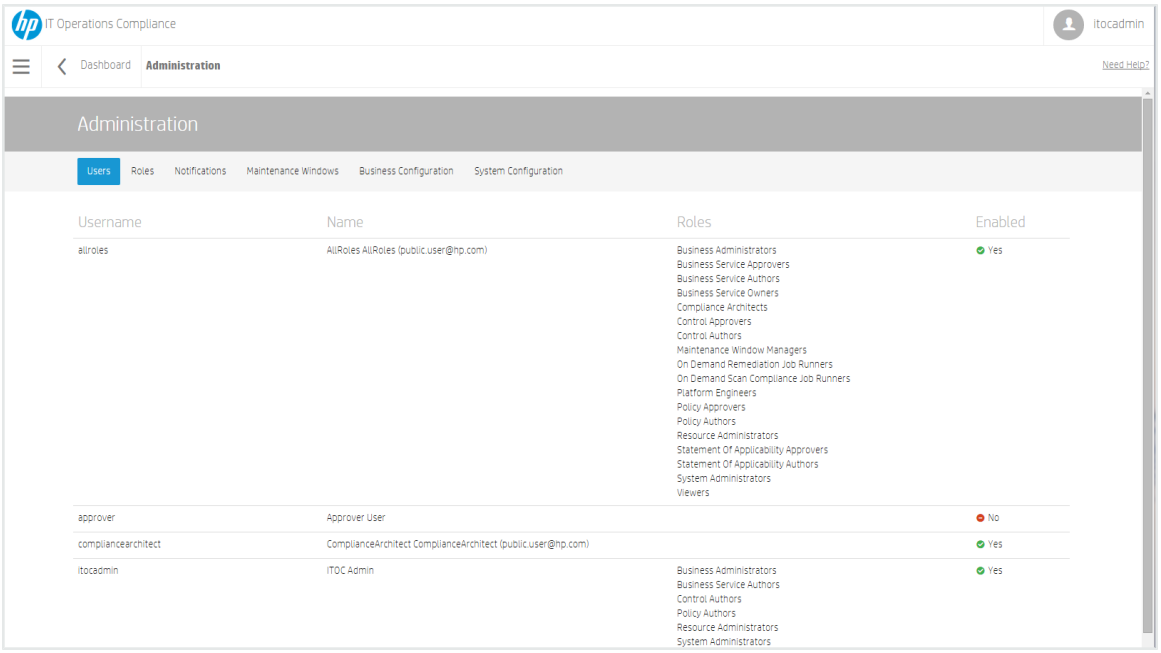
- View user profiles (see Users).
- View roles and view permissions (see Roles and Permissions).
- Manage notifications (see Notifications).
- Create, edit, and delete maintenance windows (see Maintenance Windows).
- View and edit business configuration details (see Business Configuration).
- View and edit system configuration details (see System Configuration).
- Create and edit organizations using Lightweight Directory Access Protocol (LDAP) integration (see Organizations).
- How to use the Organizations Administration User Interface (UI) (see Organizations).

View Administration in ITOC

The **Administration** view shows information about ITOC users, roles, notifications, business configuration, system configuration, and maintenance windows.

At ITOC installation, a single public provider organization is set up by default. The seeded administrator (or **itocadmin**) user has the CSA_ADMINISTRATION role and can log into the Organizations Administration UI. After the administrator integrates ITOC with LDAP, he can assign a group he has created to the administrator role, so users in that group can access the Organizations Administration UI. For more information, see Organizations.

To see the **Administration** section in the ITOC UI, a user needs to have either the **Business Administrators** or **System Administrators** role.



Users with the **Business Administrators** role can see:

- **Users** - View only for the logged-in user's organization.
- **Roles** - View only.
- **Notifications** - Editable only by a user logged in as public organization. These settings apply to all organizations.
- **Maintenance Windows** - View logged-in user's organization and public organization maintenance windows. Create, edit, and delete are available only for the logged-in user's organization.
- **Business Configuration** - Editable and set per organization.

Users with the **System Administrators** role can see:

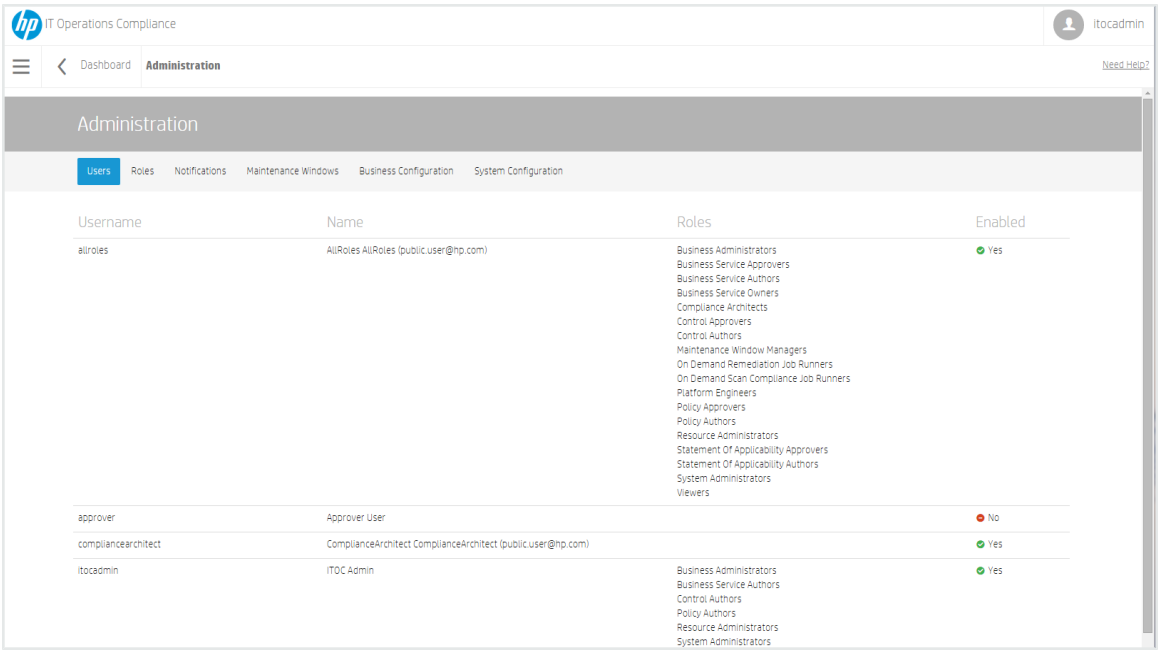
- **System Configuration** - Editable only by a user logged in as a public organization. These settings apply to all organizations.

Chapter 2 Users

ITOC provides a role-based security model that allows only authorized users to perform specific operations. The ITOC administrator user, **itocadmin**, is one of a set of OOTB ITOC seeded users described in this chapter.

View Users in ITOC

From the **Users** view, you can see all users in the system and their user names and roles. You must have the **Business Administration** role to see this view.



- **Username** - The user name.
- **Name** - Name of the user and user email address.
- **Roles** - The roles a user has in ITOC.
- **Enabled** - Whether or not this user is enabled in the system.

The following table lists ITOC seeded users.

- The password for seeded users is "hpitoc" (except **itocadmin**, for which you set the password during installation).
- After integrating with LDAP, you can disable seeded users (see Disable Seeded Users).

ITOC Seeded Users

Username	Name	Roles
approver	Approver User	• Business services approvers • Control approvers • Policy approvers • Statement of applicability (SoA) approvers
compliancearchitect	Compliance Architect	• Compliance architects
itocadmin	ITOC Administrator	• Business administrators • Business service authors • Control authors • CSA_ADMINISTRATION (visible only in the **Organizations Administration UI**) • Policy authors • Resource administrators • System administrators
jobrunner	Job Runner	• On-demand scan compliance job runners • On-demand remediation job runners
platformengineer	Platform Engineer	• Platform engineers
serviceowner	Service Owner	• Business service owners
viewer	Viewer User	• Viewers

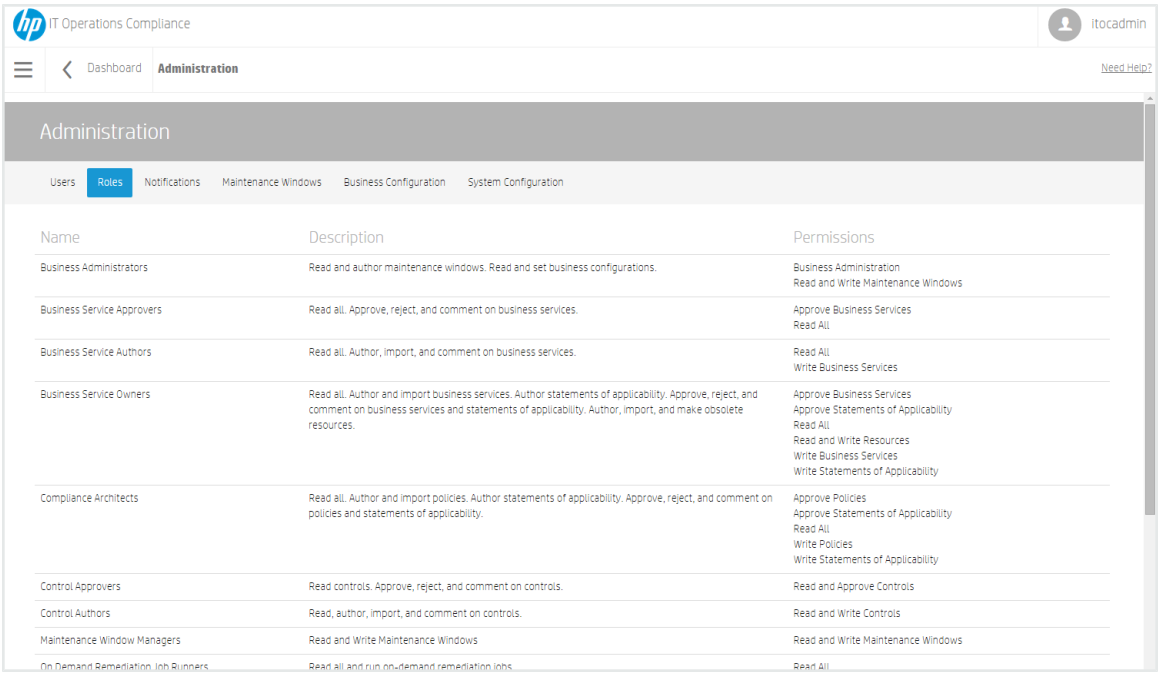
For information about integrating with LDAP and creating organizations and users, see Organizations Overview.htm.

Chapter 3 Roles and Permissions

This chapter describes ITOC roles and permissions.

Roles

A role has a name, description, and a set of permissions. Specified permissions enable the user with that role to perform tasks; for example, permissions allow compliance architects to manage ITOC policies and business service owners to manage business services and create SoAs. Roles cannot be added, edited, or deleted.



The following table shows ITOC roles, and the permissions and responsibilities of each role. A user must have the business administration role to log into ITOC to view role details.

ITOC Roles and Responsibilities

Name	Description	Permissions
Business Administrators	• Read and author maintenance windows. • Read and set business	• Read and Write Maintenance Windows • Business Admin-

Name	Description	Permissions
	configurations.	istration
Business Service Approvers	• Read all. • Approve, reject, and comment on business services.	• Read All • Approve Business Services
Business Service Authors	• Read all. • Author, import, and comment on business services.	• Read All • Write Business Services
Business Service Owners	• Read all. • Author and import business services. • Author SoAs. • Approve, reject, and comment on business services and SoAs. • Author, import, and make obsolete resources.	• Read All • Write Business Services • Write Statements of Applicability • Approve Business Services • Approve Statements of Applicability • Read and Write Resources
Compliance Architects	• Read all. • Author and import policies. • Author SoAs. • Approve, reject, and comment on policies and SoAs.	• Read All • Write Policies • Write Statements of Applicability • Approve Policies • Approve Statements of Applicability
Control Approvers	• Read controls. • Approve, reject, and comment on controls.	• Read and Approve Controls

Name	Description	Permissions
Control Authors	• Read, author, import, and comment on controls.	• Read and Write Controls
Maintenance Window Managers	• Read and write maintenance windows.	• Read and Write Maintenance Windows
On Demand Scan Compliance Job Runners	• Read all. • Run on-demand scan compliance jobs.	• Read All • Run Scan Compliance Job
On Demand Remediation Job Runners	• Read all. • Run on-demand remediation jobs.	• Read All • Run Remediation Job
Platform Engineers	• Read, author, and import controls. • Approve, reject, and comment on controls.	• Read and Write Controls • Read and Approve Controls
Policy Approvers	• Read all. • Approve, reject, and comment on policies.	• Read All • Approve Policies
Policy Authors	• Read all. • Author, import, and comment on policies.	• Read All • Write Policies
Resource Administrators	• Read, author, import, and make obsolete resources.	• Read and Write Resources
Statement of Applicability Approvers	• Read all. • Approve, reject, and comment on SoAs.	• Read All • Approve Statements of Applicability
Statement of Applicability Authors	• Read all. • Author, approve,	• Read All • Approve Statements of

Name	Description	Permissions
	reject, and comment on SoAs.	Applicability • Write Statements of Applicability
System Administrators	• Read and set system configurations.	• System Administration
Viewers	• Read business services, controls, resources, policies, and SoAs.	• Read All

Permissions

Permissions define the action (such as scan, remediate, or import) that can be taken against an object type. Permissions cannot be added, edited, or deleted.

ITOC Permissions

Permission Name	Permission Description
Approve Business Services	• Approves business services. • Rejects business services. • Comments on business services. • Requires **Read All** permission.
Approve Policies	• Approves policies. • Rejects policies. • Comments on policies. • Requires **Read All** permission.
Approve Statements of Applicability	• Approves SoAs. • Rejects SoAs. • Comments on SoAs. • Requires **Read All** permission.

Permission Name	Permission Description
Business Administration	• Sets compliance threshold. • Sets business object ID prefixes. • Sets workflows. • Configures notifications.
Read All	• Views policy properties, requirements, rules, and compliance score. • Views business service properties (including default maintenance windows), topology, and compliance score. • Views SoA properties (including maintenance windows), exceptions, and compliance score. • Views control properties and scripts. • Views IT resource properties. • Reads maintenance windows from the business service or SoA associated with a specified window.
Read and Approve Controls	• Views control properties, scripts, and parameters. • Approves on controls. • Rejects on controls. • Comments on controls.
Read and Write Controls	• Views control properties, scripts, and parameters. • Creates controls. • Imports controls. • Edits control properties, scripts, and parameters. • Comments on controls. • Submits controls. • Makes controls obsolete.
Read and Write Maintenance Windows	• Read maintenance windows.

Permission Name	Permission Description
	• Create maintenance windows. • Edit maintenance windows. • Delete maintenance windows.
Read and Write Resources	• Views resources and compliance score. • Creates resources. • Imports resources. • Edits resources. • Makes resources obsolete. • Installs agents.
Run Remediation Jobs	• Runs on-demand remediation jobs. • Requires **Read All** permission.
Run Scan Compliance Jobs	• Runs on-demand scan compliance jobs. • Requires **Read All** permission.
System Administration	• Sets system configurations. • Sets up email integration with SMTP. • Sets schedule for recompliance calculation. • Sets schedule for user to perform LDAP synchronization.
Write Business Services	• Creates new business services or new draft revisions. • Imports new business services. • Edits business services properties and topology. • Comments on business services. • Submits business services. • Makes business services obsolete. • Requires **Read All** permission.
Write Policies	• Creates new policies or new draft revisions.

Permission Name	Permission Description
	• Imports policies. • Edits policy properties, requirements, and rules. • Comments on policies. • Submits policies. • Makes policies obsolete. • Requires **Read All** permission.
Write Statements of Applicability	• Creates new SoAs and new draft revisions. • Edits SoA properties and exceptions. • Assigns maintenance windows to SoAs. • Comments on SoAs. • Submits SoAs. • Makes SoAs obsolete. • Requires **Read All** permission.

Chapter 4 Notifications

Users are notified by email when they need to perform actions (such as approve a revision) or when changes occur to an object that is of interest to them. A user logged into the public organization with the **Business Administration** permission can view and manage notifications.

The administrator can enable or disable notification types, such as notification of a new revision of an object being promoted into production. The administrator also customizes whom to notify per notification type, such as notifying the named **Approver** user when an object revision is submitted for that user's approval.

Notifications Overview

ITOC has several notification types, all of which are enabled by default. Email notifications are triggered by a specific event, such as submitting an object revision for approval.

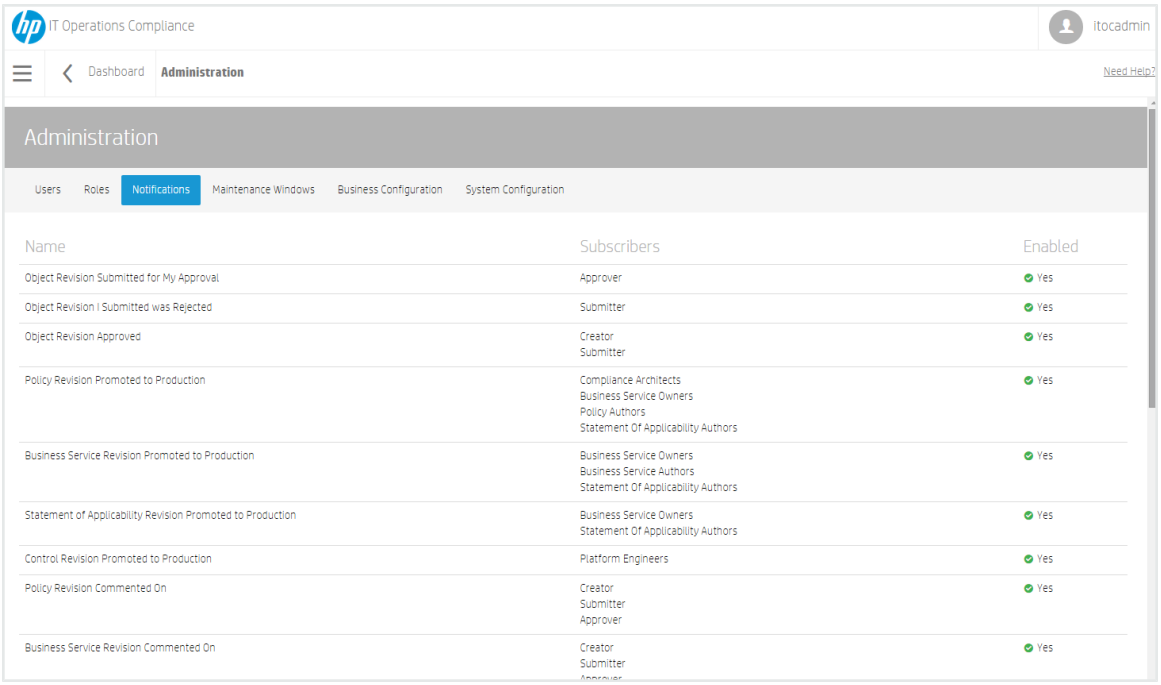
Subscribers

Each notification type has a default set of subscribers. The subscribers receive notifications based on their action on the object revision that the notification is about. Possible **Subscriber** options are:

- **Creator** - The user who created the object revision.
- **Submitter** - The user who submitted the object revision.
- **Approver** - The user specified as the approver for the object revision.
- **Rejecter** - The user who rejected the object revision.
- **Commenter** - The user who commented on the object revision.
- One of 18 fixed **Roles** (see Roles). If a role is selected, the notification is sent to all users who have that particular role.

View Notifications

A user with the **Business Administration** permission can log into any organization to view notifications. The **Notifications** view shows the notification types and subscribers in the ITOC system:



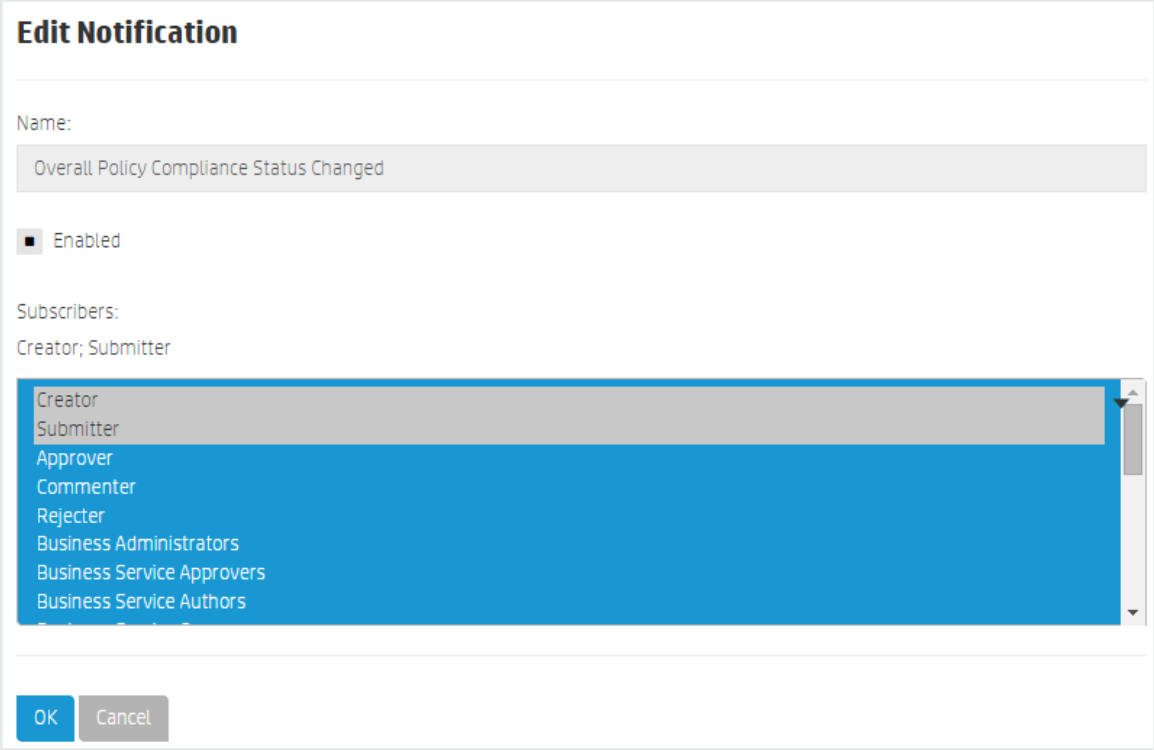
From here, you can view:

- **Name** - Notification type.
- **Subscribers** - Roles of users who receive notifications (**Creator**, **Submitter**, **Approver**, **Rejecter**, **Commenter**).
- **Enabled** - Whether or not a notification type is enabled.

Edit Notifications

The user with Business Administration permission in a public organization can modify the subscribers list and change a notification's enabled/disabled state. To edit notifications:

1. Navigate to the **Notifications** list.
2. Click a notification name. The **Edit Notification** dialog appears, with the current information for the notification already selected:



- **Name** - View only.
- **Enabled** - Checkbox for the enabled state.
- **Subscribers:** - List of subscriber roles, with the current subscriber roles selected (**Creator** and **Submitter** in the example).

3. Press **OK**.

Configure SMTP for Notifications

You must configure your SMTP server to send notifications. See System Configuration for configuration details.

Notification Types

Event-Driven Types

Notifications are triggered by an event, such as an object revision being promoted to production. This section describes notification types.

Business Service Revision Commented On

When a user comments on a business service revision, a notification email is sent to the **Creator**, **Approver** (if applicable), and **Submitter** (if applicable).

Business Service Revision Promoted to Production

When a business service revision is promoted to production, a notification email is sent to **Business Service Authors**, **Business Service Owners**, and **Statement of Applicability Authors**.

Business Service Revision Promoted to Production, where Business Service is Associated with an SoA

When a business service revision is promoted to production and an SoA is associated with it, a notification email is sent to the **Creator** and **Submitter** of the SoA and **Submitter** of the business service.

Business Service was Obsoleted

When a business service becomes obsolete, a notification email is sent to **Business Service Authors**, **Business Service Owners**, and **Statement of Applicability Authors**.

Control Revision Commented On

When a user comments on a control revision, a notification email is sent to the **Creator**, **Approver** (if applicable), and **Submitter** (if applicable).

Control Revision Promoted to Production

When a control revision is promoted to production, a notification email is sent to **Platform Engineers**.

Control Revision Promoted to Production, where Control used in a Policy Rule

When a control revision that is used in a policy rule is promoted to production, a notification email is sent to the **Creator** and **Submitter** of the policy and **Submitter** of the control.

Control Revision Promoted to Production, where Control used in a Policy Rule, and Policy is associated with an SoA

When a control revision that is used in a policy rule is promoted to production and the policy is associated with an SoA, a notification email is sent to the **Creator** and **Submitter** of the SoA and **Submitter** of the policy.

Control was Obsoleted

When a control becomes obsolete, a notification email is sent to **Compliance Architects**, **Control Authors**, **Platform Engineers**, and **Policy Authors**.

Maintenance Window was Deleted and Auto-removed from SoA

When a maintenance window is deleted and automatically removed from an SoA, a notification email is sent to the **Creator** and **Submitter** of the SoA.

Object Revision Approved

When an object revision is approved, a notification is sent to the **Submitter** and **Creator**.

Object Revision Submitted for My Approval

When a user submits an object revision that requires approval, a notification email is sent to the **Approver**.

Note: HP recommends you retain the default subscriber, because the message will not make sense to any other user.

Object Revision I Submitted was Rejected

When an object revision a user submits is rejected, a notification email is sent to the **Submitter**.

Note: HP recommends you retain the default subscriber, because the message will not make sense to any other user.

Policy Revision Commented On

When a user comments on a policy revision, a notification email is sent to the **Creator**, **Approver** (if applicable), and **Submitter** (if applicable).

Policy Revision Promoted to Production

When a policy revision is promoted to production, a notification email is sent to **Business Service Owners**, **Compliance Architects**, **Policy Authors**, and **Statement of Applicability Authors**.

Policy Revision Promoted to Production, where Policy is Associated with an SoA

When a policy revision is promoted to production and an SoA is associated with it, a notification

email is sent to the **Creator** and **Submitter** (of the SoA) and **Submitter** of the policy.

Policy Revision Promoted to Production, which Invalidated an SoA Exception

When a policy revision is promoted to production, causing an SoA exception to become invalidated by deleting the excepted requirement, a notification email is sent to the **Creator** and **Submitter** of the SoA and **Submitter** of the policy.

Policy was Obsoleted

When a policy becomes obsolete, a notification email is sent to **Compliance Architects**, **Policy Authors**, and **Statement of Applicability Authors**.

Resource was Obsoleted

When a resource becomes obsolete, a notification email is sent to **Business Service Authors**, **Business Service Owners**, and **Resource Authors**.

Statement of Applicability Revision Commented On

When a user comments on an SoA revision, a notification email is sent to the **Creator**, **Approver** (if applicable), and **Submitter** (if applicable).

Statement of Applicability Revision Promoted to Production

When an SoA revision is promoted to production, a notification email is sent to **Statement of Applicability Authors** and **Business Service Owners**.

Statement of Applicability Revision was Obsoleted

When an SoA revision becomes obsolete, a notification email is sent to **Statement of Applicability Authors** and **Business Service Owners**.

Reminder Types

Reminder types in ITOC have one of two global reminder frequency values:

- The number of days before an event (for example, the number of days before an exception expires).
- The number of days after an event (for example, number of days after a revision was submitted for approval). This reminder will be sent up to 3 times. For example, if a reminder is

set to send 7 days after a reminder, it will send 7, 14, and 21 days after, if necessary.

These setting are set at a system level. For more information, see System Configuration.

This section lists reminder types.

Draft Revision In Draft State for N Days

When an draft object revision has been in draft state for a specified number of days, a notification email is sent to the **Creator**.

Object Revision Has Been Awaiting My Approval

When an object revision has not been approved for a specified number of days after its due date, a notification email is sent to the **Approver**.

Object Revision I Submitted Has Not Been Approved

When an object revision you have submitted has not been approved for a specified number of days after its due date, a notification email is sent to the **Submitter**.

Policy Effective Date Is Coming Up Soon

When a policy effective date is coming up in a specified number of days, a notification email is sent to the **Approver** and **Submitter**.

Production SoA With Expired Exception(s)

When a production SoA has exception(s) that have expired, a notification email is sent to the **Submitter**.

SoA Revision Has Exception(s) Expiring Soon

When an SoA revision has exception(s) that are due to expire in a specified number of days, a notification email is sent to the **Submitter**.

Compliance Status

Business Service Meeting MSLO Changed

When a business service revision has a change in MLSO status, a notification email is sent to the **Creator** and **Submitter** of the business service.

Business Service Meeting RSLO Changed

When a business service revision has a change in RLSO status, a notification email is sent to the **Creator** and **Submitter** of the business service.

Overall Business Service Compliance Status Changed

When the overall business service compliance status changes, a notification email is sent to the **Creator** and **Submitter** of the policy.

Overall Policy Compliance Status Changed

When the overall policy compliance status changes, a notification email is sent to the **Creator** and **Submitter** of the policy.

Remediation Job Completed

When a remediation job for an SoA completes, a notification email is sent to the **Creator** and **Submitter** of the SoA.

Scan Job Completed

When a compliance scan for an SoA completes, a notification email is sent to the **Creator** and **Submitter** of the SoA.

Chapter 5 Maintenance Windows

ITOC manages business service availability through the use of maintenance windows. Maintenance windows enable your ITOC system to run scan compliance and remediation jobs automatically, which keeps all SoAs in the system meeting their SLOs.

Maintenance Windows Overview

A maintenance window defines a block of time in which jobs are allowed to run and which types of jobs can run in the window. You can use a maintenance window to define a recurring maintenance schedule or a single-occurrence maintenance window. Each instance when a maintenance window is active is called a timeslot.

The ITOC administrator defines the set of allowable maintenance windows, and the business service owner associates a business service with a set of maintenance windows per SoA. The business service owner assigns maintenance windows to an SoA based on availability of a business service for the scan or remediation jobs, with enough frequency (timeslots) to meet SLOs. For example, if an MSLO is within two weeks, the business service owner will not use a monthly scan window, because the SoA will constantly fall out of MSLO.

Common examples of defined maintenance schedules are:

- Saturday from 2-6 AM Pacific Time (remediate)
- Mondays, Wednesdays, and Fridays from 1-5AM Pacific Time (scan only)
- Sunday, February 1, 2015, from 2-5AM Pacific Time (scan and remediate)

Maintenance Window Work Prioritization

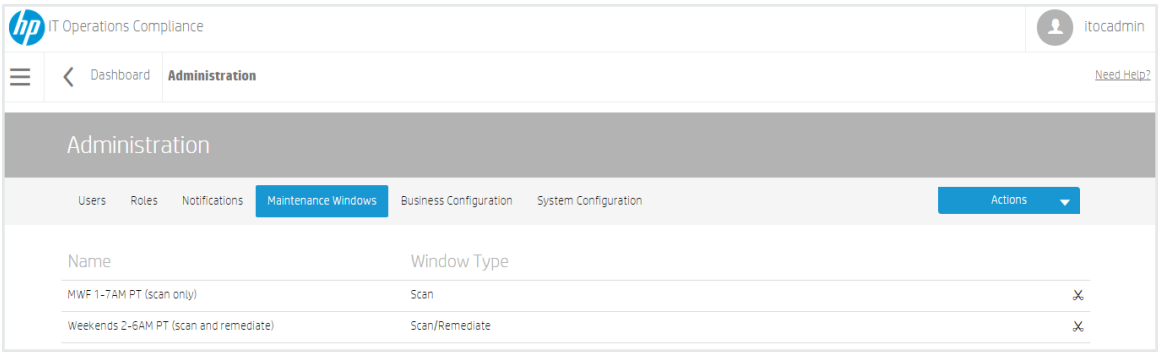
When a maintenance window timeslot begins, the system automatically determines the SoAs on which to run jobs by getting all SoAs with that maintenance window assigned. The system uses this data to identify and prioritize work to be done.

When multiple SoAs are assigned to one maintenance window, the maintenance window work is prioritized on the business service priority (e.g., Gold, Silver, or Bronze) and optimized to meet MSLO.

The system optimizes the scans to meet MSLO. If the SoA has already been scanned within the first half of the MSLO period, then the data is considered fresh enough that no additional scan is needed. For example, the SoA is in a daily maintenance window, and the MSLO is within 30 days. It may not be scanned in every timeslot.

View Maintenance Windows

To view maintenance windows in ITOC, navigate to the **Maintenance Windows** tab in **Administration**:



This page shows a list of maintenance windows:

- **Name** - Name of the maintenance window.
- **Window Type** - **Remediate**, **Scan**, or **Scan and Remediate**.

If you are logged into a consumer organization, you can also see the public organization maintenance windows.

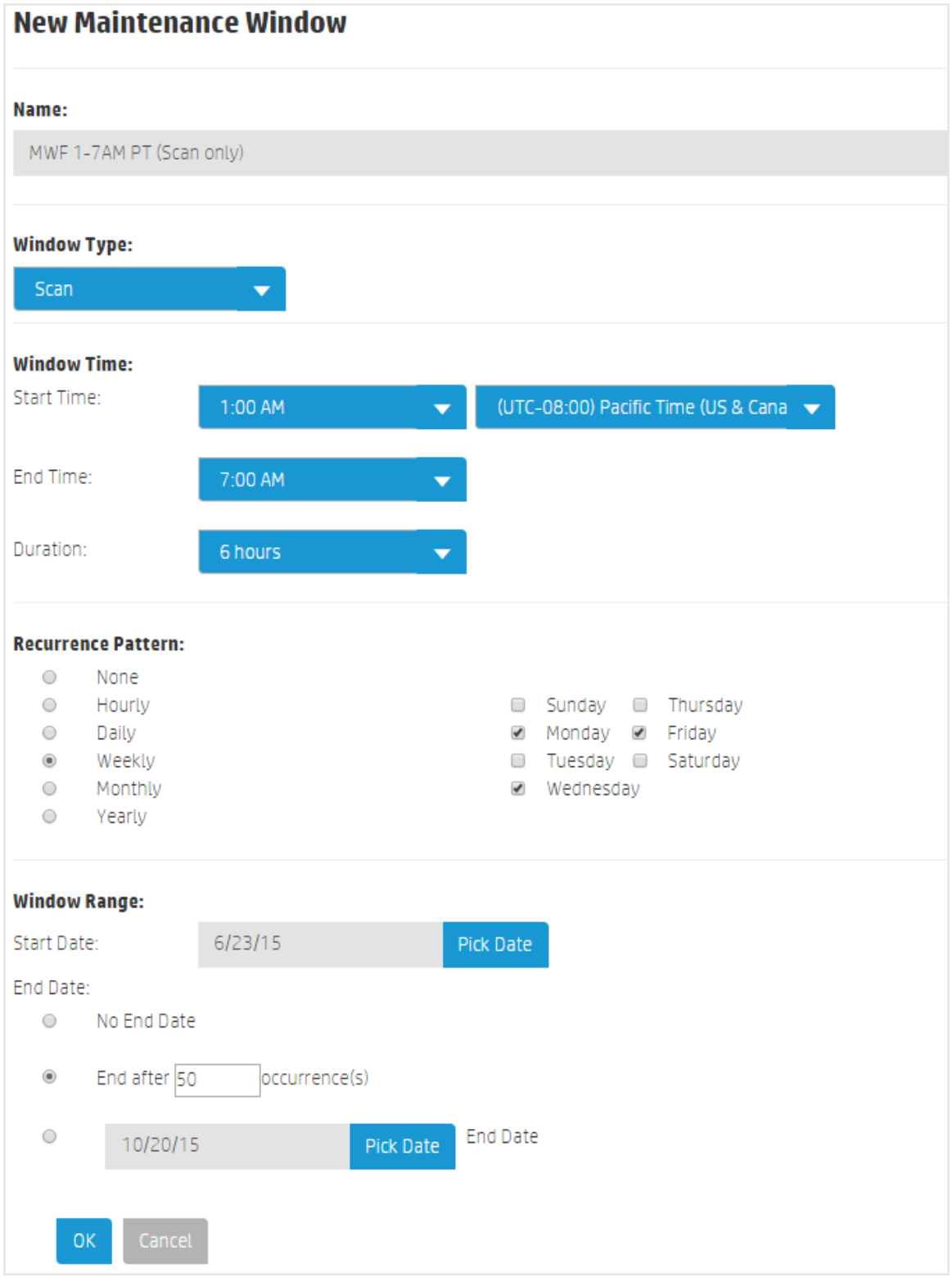
Create a New Maintenance Window

To create a new maintenance window in an organization, the user must be logged in to the specified organization with the Read and Write Maintenance Windows permission.

Perform the following steps to create a new maintenance window:

1. Navigate to the **Maintenance Windows** tab in **Administration**.
2. From **Actions**, select **New Window**.

3. The **New Maintenance Window** screen appears:



Complete the following fields:

- **Name:** Name of the maintenance window.

  Business owners will select this maintenance window from several maintenance windows in the SoA. In order for business owners to identify and select the correct maintenance window, provide a unique descriptive name, including a summary of the schedule, the timezone, and window type.

- **Window Type:** Determines what types of jobs are allowed to run in the window. Select a window type:

  - **Remediate** - Only **Run Remediation** jobs can run in the window.
  - **Scan** (default) - Only **Scan Compliance** jobs can run in the window.
  - **Scan/Remediate** - Either **Scan Compliance** or **Run Remediation** jobs can run in the window.

- **Window Time**

  - **Start Time:** Select a time of day from the first dropdown list (default is 12 AM), and select a timezone from the second dropdown list [default is (UTC-08:00) Pacific Time (US & Canada)].

    Note: Some timezones are affected by daylight savings time.

  - **End Time:** Select a time of day from the first dropdown list (default is 12 AM).
  - **Duration:** Length of time (default is 0 minutes).

- **Recurrence Pattern:** Select a recurrence pattern:

  - **None** - No recurrence pattern selected.
  - **Hourly** - Repeats at the specified frequency within a single day. For example, if a maintenance window is scheduled to start at 2 a.m. and run for 4 hours and the recurrence pattern is hourly every 8 hours, it will run from 2 to 6 a.m., 10 a.m. to 2 p.m., and 6 p.m. to 10 p.m.
  - **Daily** (default) - Runs once every day.
  - **Weekly** - You can specify any or all days of the week.

- **Monthly** - You can specify one of the following:
  - The <n> day of every <n> month - for example, **Day 1 of every 3 Month(s)**, or
  - The <n> <weekday> of every <n> month - for example, **Second Monday of every 3 Month(s)**.
- **Yearly** - You can specify one of the following:
  - The <month> and <day> to run on annually - for example, **Every July 10th**, or
  - The <n> <weekday> of a selected month annually - for example, **The Second Friday of July**.

- **Window Range:**
  - **Start Date:** Use the **Pick Date** dropdown calendar to select a start date. The default is today's date.
  - **End Date:**
    - **No End Date** - This radio button is selected by default.
    - **End after 50 occurrence(s)** - Enter a number of occurrences. The default is 50 occurrences.
    - Use the **Pick Date** dropdown calendar to select an end date. The default is today's date.

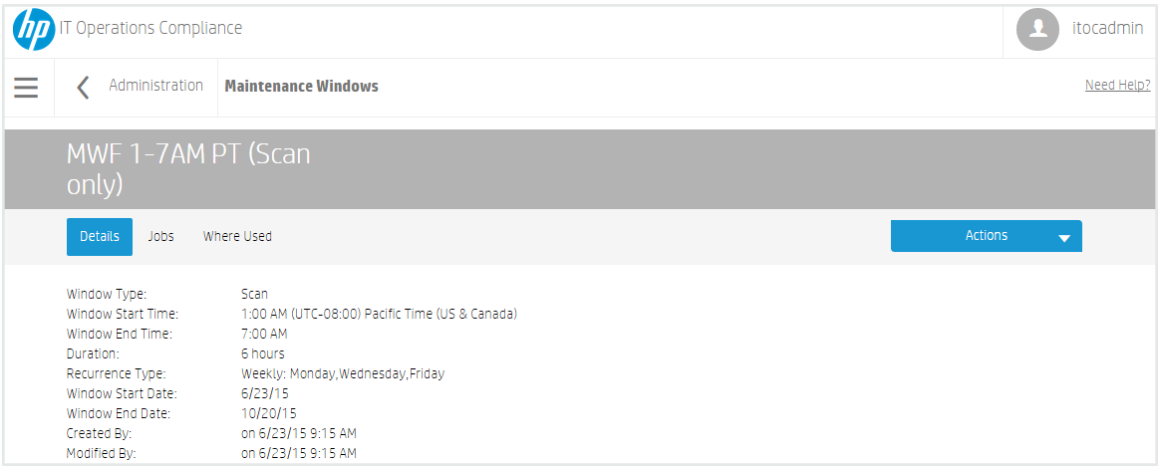
4. Press **OK** to create the maintenance window.

Manage Maintenance Windows

To update and manage maintenance windows in an organization, the user must be logged in to the specified organization with the **Read and Write Maintenance Windows** permission.

Maintenance Windows Details

From the **Maintenance Windows** list, click on the name of the maintenance windows whose details you want to view:



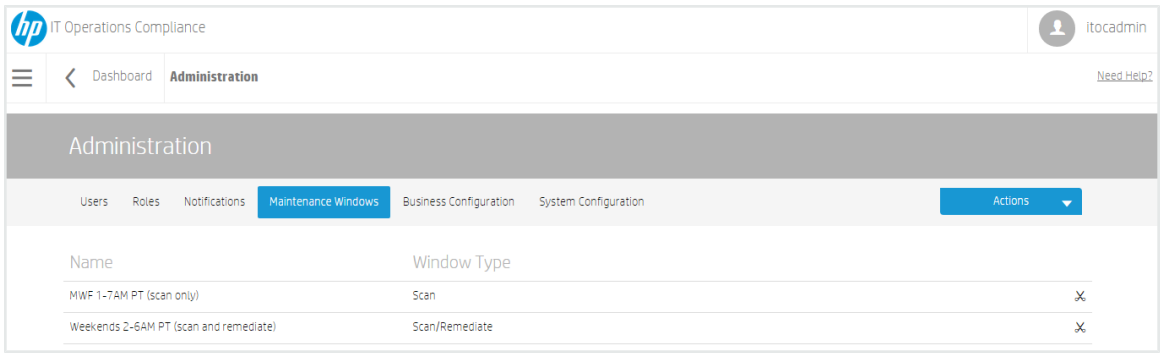
To edit maintenance windows properties...

1. Click Actions to select **Edit Properties**.
2. Modify the maintenance window as needed.
3. Press **OK**.

   A maintenance window cannot be modified while it is starting a new timeslot; if it is, an "in use" exception occurs. If this exception occurs, the user must wait to continue until after the maintenance window has finished starting its work.

To delete a maintenance window...

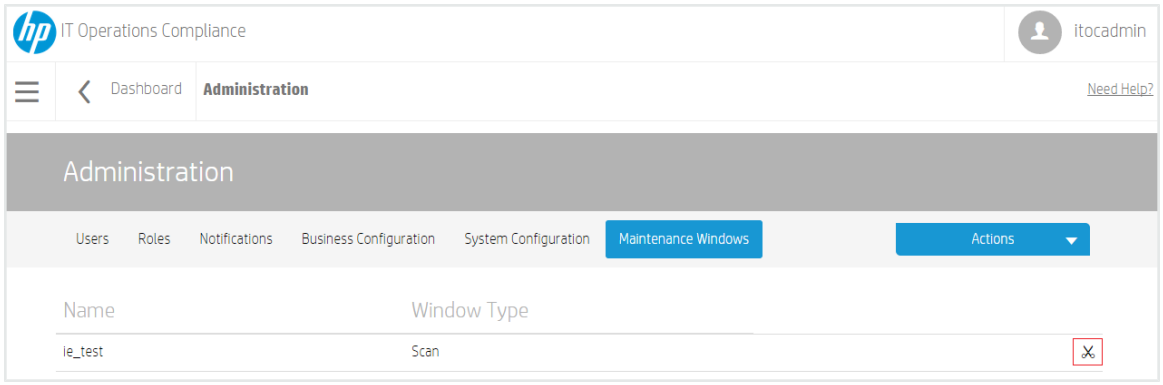
1. Click on the maintenance window you want to delete, and click **Actions**:



2. Select **Delete Maintenance Window**.
3. From the confirmation dialog that appears, press **Yes**.

   Or:

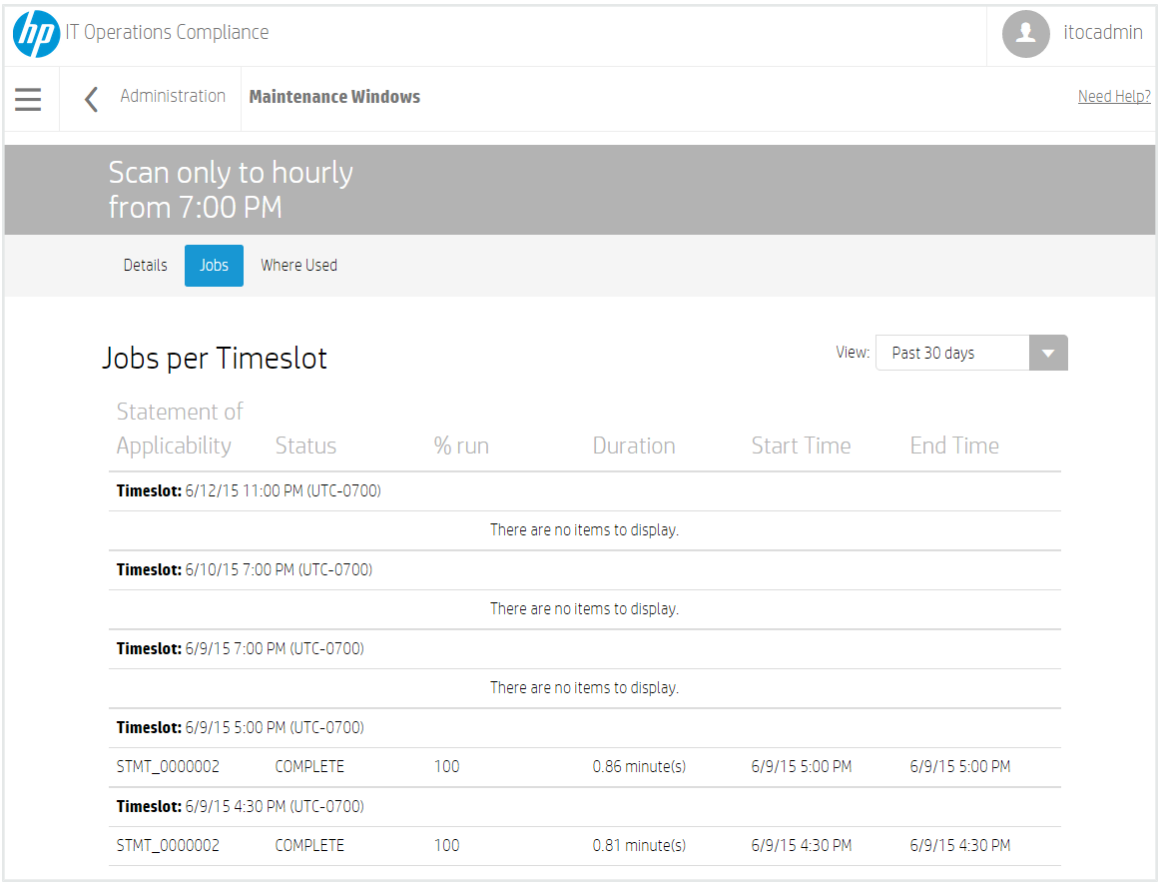
1. Press the icon in the row of the maintenance window you want to delete:



2. From the confirmation dialog that appears, press **Yes**.

Maintenance Windows Jobs

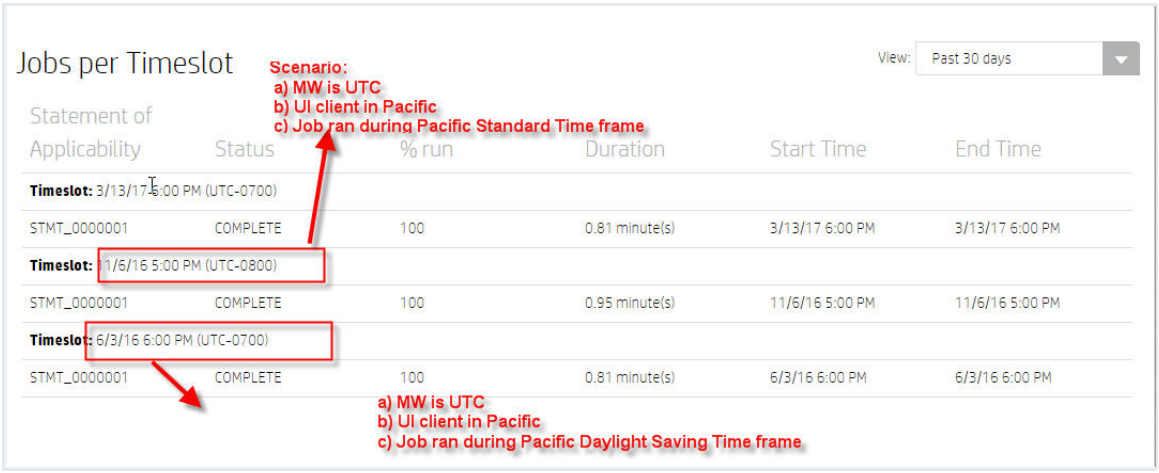
Select **Jobs** to view the **Jobs per Timeslot** for this maintenance window:



From **View:**, you can filter jobs per timeslot by **Past 30 days** (default), **Past 60 days**, **Past 90 days**, and **All**.

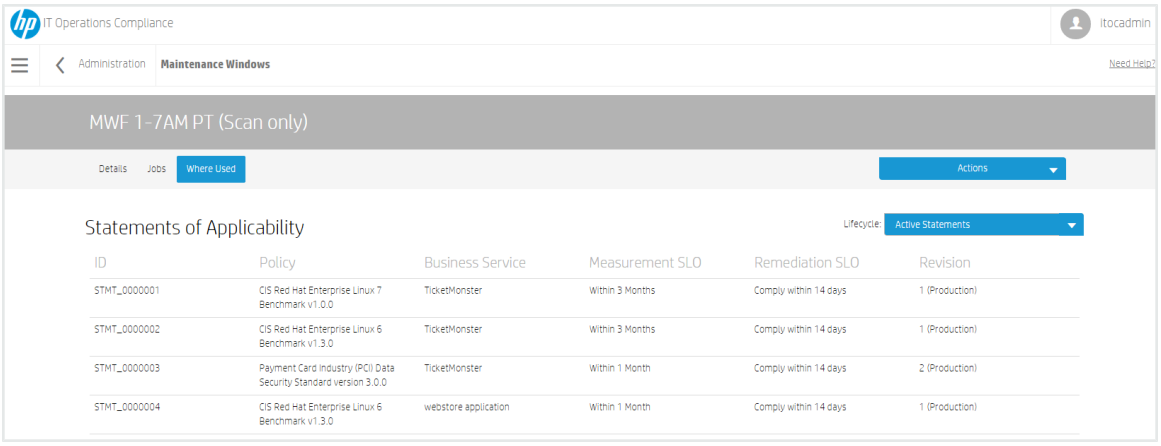
- **ID** - IDs of each SoA on which a job was run during the specified maintenance window timeslot.
- **Status** - Status of the job that was run during the specified maintenance window timeslot:
  - **PENDING**: The maintenance window timeslot has started and is planning work. Job is pending execution.
  - **IN PROGRESS**: The maintenance window timeslot has started and is executing the job.
  - **COMPLETE**: The job has completed execution.
  - **INCOMPLETE**: The maintenance window timeslot ended before the job was executed completely.
- **% run** - Percentage of work that was executed in the job.
- **Duration** - Length of time it took the job to run.
- **Start Time** - The start time of the job.
- **End Time** - The end time of the job.

In the following example, the maintenance window is set to Pacific Time, which is daylight savings time-aware. The maintenance window starts at UTC-7 when daylight savings time is active, and UTC-8 when daylight savings time is not active:



Maintenance Windows Where Used

Select **Where Used** to see the SoAs in which a specific maintenance window is used:



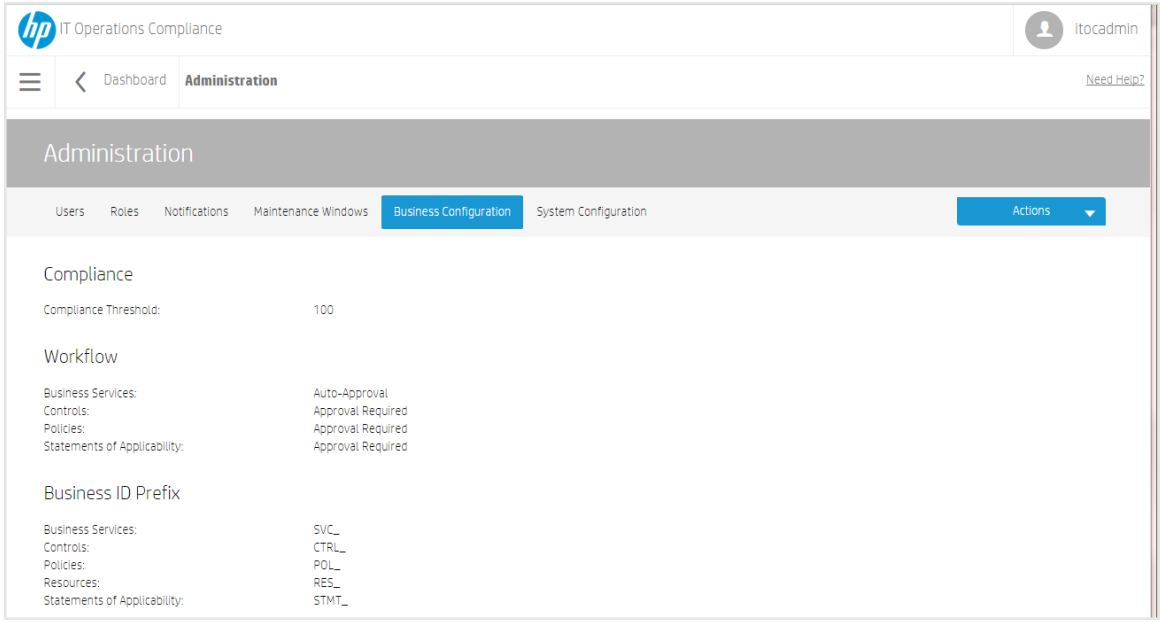
- **ID** - The SoA ID.
- **Policy** - The policy associated with the SoA.
- **Business Service** - The business service associated with the SoA.
- **Measurement SLO** - The MSLO defined by the SoA.
- **Remediation SLO** - The RSLO defined by the SoA.
- **Revision** - The SoA revision and lifecycle state.

Chapter 6 Business Configuration

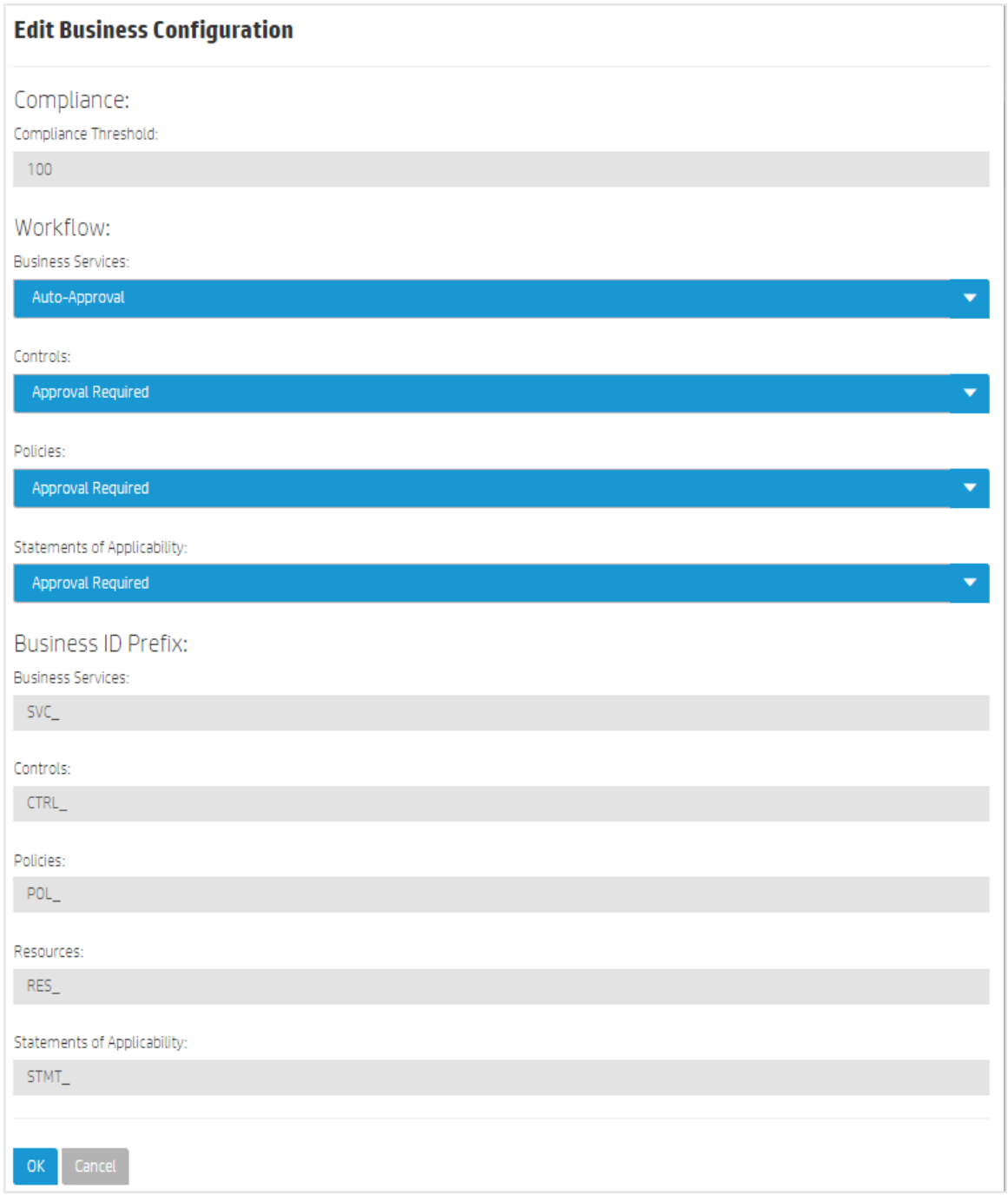
To view business configuration details, the user must be logged in with the Business Administration role.

Perform the following steps to view and edit business configuration details:

1. Log into ITOC and click the **Administration** tab.
2. Click the **Business Configuration** tab to view details.



3. Click **Actions** to **Edit Business Configuration**. The **Edit Business Configuration** form appears:



4. Modify information as needed, and press **OK**.

> **Note:** Changes made apply to the organization to which the business administrator is logged in.

Compliance

- **Compliance Threshold:** The value can be a number from 1 through 100. It is the minimum percentage of compliance to be considered compliant overall. The default is 100.

Workflow

Set the workflow per business entity. **Auto-Approval** means that no approval is required, and submit takes the entity from draft to production. **Approval Required** means that the named approver must approve object before going into production.

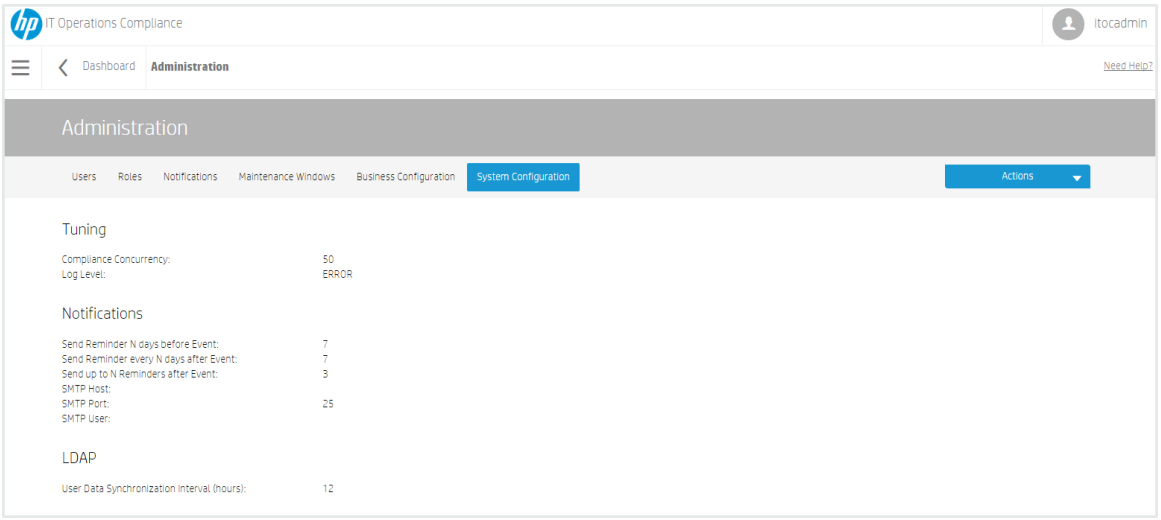
- **Business Services:** Default is Auto-Approval.
- **Controls:** Default is Approval Required.
- **Policies:** Default is Approval Required.
- **Statements of Applicability:** Default is Approval Required.

Business ID Prefix

Per business entity, define the starting characters for the ID to distinguish different entity types from each other. The user can change the prefix of the auto-generated ID for each object type. The allowable prefix length is 1 to 50 characters.

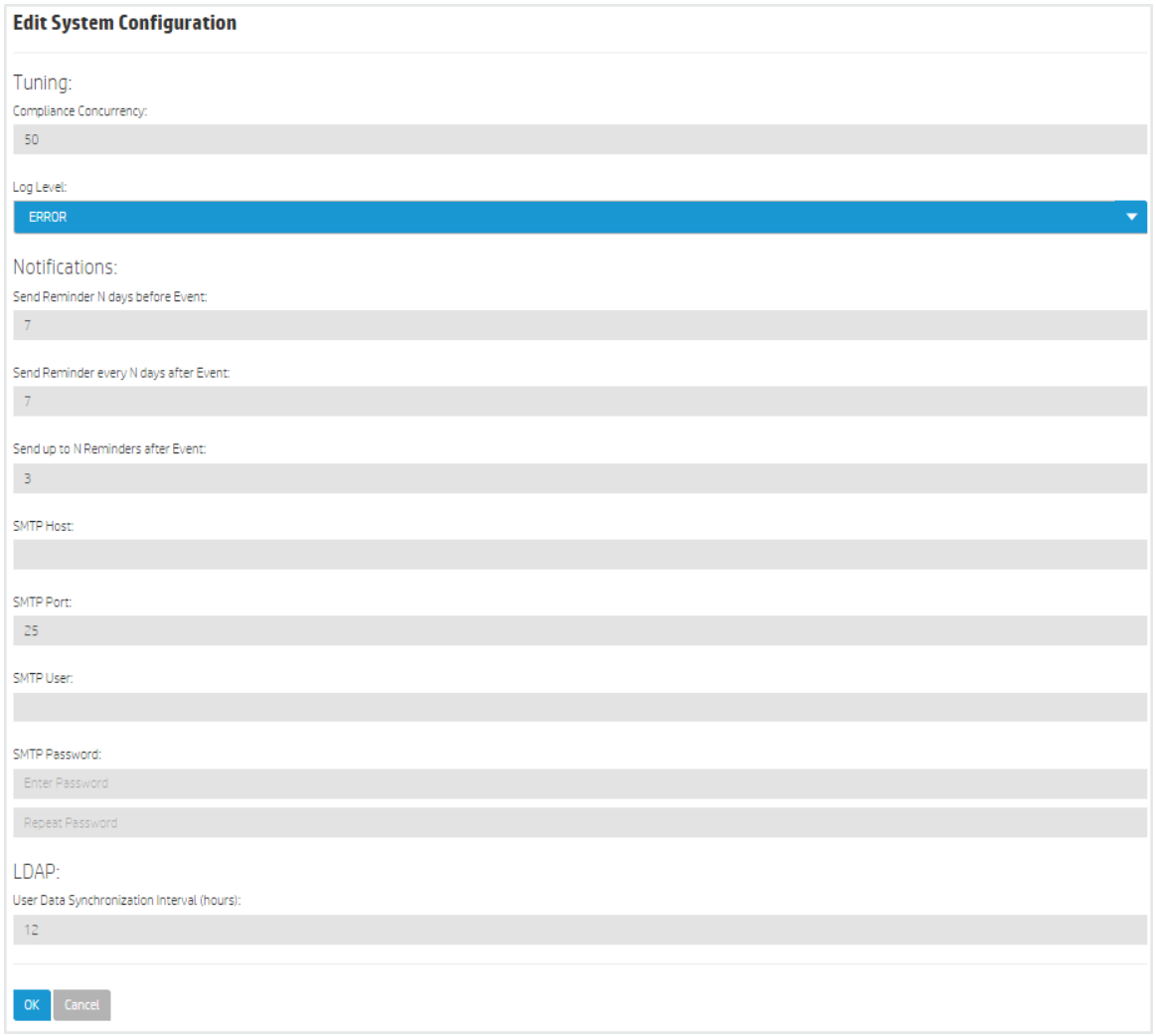
Chapter 7 System Configuration

To view and modify system configuration details, the user must be logged in as **Public Organization** and have the **System Administration** permission. To view system configuration settings only, the user can log in with the **System Administration** role.



To modify system configuration:

1. Click **Actions** to **Edit System Configuration**. The **Edit System Configuration** dialog appears:



Tuning

- **Compliance Concurrency** - Number of concurrent threads used during Scan Compliance and Remediate job execution. The user can modify the compliance concurrency to any value from 1 through 255. The default is 50.
- **Log Level**: Set the log level to control the logging granularity in the `<install directory>/serverlog/itoc-server.log`. Available levels are **ALL**, **DEBUG**, **ERROR** (default), **INFO**, **OFF**, **TRACE**, and **WARN**.

Notifications:

- **Set Reminders N Days Before Event:** - The default is 7 (see Reminder Types).
- **Set Reminder Every N Days after Event:** - The default is 7.

- **Send up to N Reminders After Event:** - The default is 3.
- **SMTP Host:** - Your SMTP server (e.g., smtp.yourserver.com). This field is required to enable notifications.
- **SMTP Port:** - The port configured on the SMTP server. The default is 25. This field is required to enable notifications.
- **SMTP User:** - The SMTP user. This field is used or not based on your SMTP server setup.
- **SMTP Password:** - The password must be encrypted. This field is used or not based on your SMTP server setup.

LDAP:

- **Sync User Info every N Hours:** - How often LDAP synchronization is performed. The default is 12 hours.

2. Press **OK**.

Chapter 8 Organizations

ITOC has two types of organizations – public and consumer. This chapter discusses ITOC organizations, Lightweight Directory Access Protocol (LDAP) integration, and the Organizations Administration UI.

Organizations Overview

An organization determines a user's entry point into the ITOC system and associates its users with services and resources. The ITOC administrator creates and edits user groups and assigns roles to these user groups, based on LDAP groups. Membership in an organization is determined by the organization's LDAP directory.

ITOC has two types of organizations:

- Public Provider Organizations - The provider organization hosts ITOC, manages consumer organizations, and manages resources and services. Production revisions of public objects and resources in the public provider organization are shared with the consumer organizations. For example, a user can import control and policy content from HPLN into the public provider organization. Then, each consumer organization can use these policies; for example, measure the compliance of their business services against shared or common policies.
- Consumer Organizations - The consumer organization subscribes to or consumes the resources and services provided by the provider organization. There may be multiple consumer organizations configured by the provider organization. However, each consumer or subscriber sees only the information of the consumer organization of which he is a member (membership to a consumer organization is determined by the LDAP configuration of the consumer organization).

The administrator configures ITOC to access an LDAP server, at which point LDAP users can log into the ITOC UI. LDAP authenticates user login credentials by verifying that the user name and password match an existing user in the LDAP directory.

Public Provider Organizations

At installation, one public provider organization is set up by default; no other provider-type organizations can be created. The Administrator (or **itocadmin**) user has the CSA_ ADMINISTRATION role and can log into the Organizations Administration UI. This user can:

- **Configure LDAP** - For each organization, the Administrator can specify the LDAP end-point to access as the source for users.
- **Creates one or more groups** - Each group is a representation of an LDAP group.
- **Assign roles to groups** - Assigns roles to each group (see Roles).

Consumer Organizations

Consumer organizations have the same functionality as public provider organizations. What a user can do within a consumer organization is based on the roles assigned to that user.

You can create separate consumer organizations based on your company's organizational structure.

- For example, you might create separate consumer organizations for R&D and Finance. R&D can only see R&D objects within its consumer organization plus public content; Finance can only see Finance objects within its consumer organization plus public content.
- Each organization can set different business configurations - for example, the R&D compliance threshold is set to 95, while the Finance compliance threshold is set to 100.
- Each organization can have different business processes - for example, R&D may choose to use the Auto-Approval workflow for all object types, while Finance may choose to use the Approval Required workflow.

Log Into the Organizations Administration UI

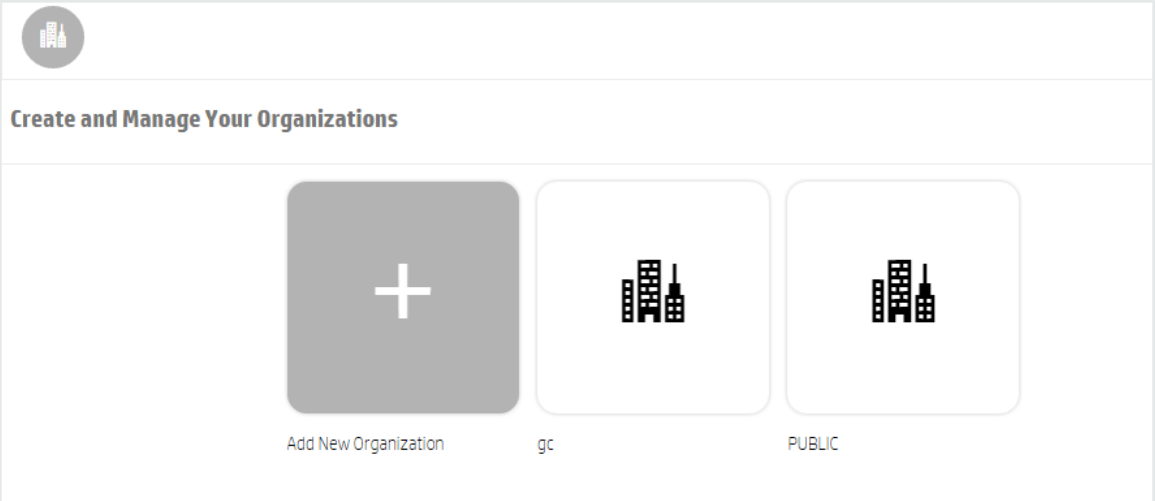
A user with the CSA_ADMINISTRATION role logs in to the **Organizations Administration UI** using port 9200. For example:

```
https://<ITOC_hostname>:9200
```

The **Create and Manage Your Organizations** view appears.

Create and Manage Organizations

At ITOC installation, a single public organization is set up. Use the **Create and Manage Your Organizations** Administration UI to create consumer organizations, as needed.



From this view, you can:

- **Add a new organization** - Click **Add New Organization**, and provide a name for the organization (see Create a New Organization for more details).
- **Navigate to an organization** - Click the tile name of the organization to which you want to navigate.

This chapter provides information about the following:

- Create a New Organization
- Configure and Manage Authentication
- Customize a Consumer Organization
- Add Groups and Associate Business Roles

Create a New Organization

The administrator can create one or many consumer organizations. Everything in production state and all resources in the public organization are shared with all consumer organizations. Objects created in consumer organizations are only known to users in that organization. Consumer organization users can use public organization objects, such as shared controls, policies, and resources.

Authentication, **Groups**, and **Business Roles** need to be configured for each organization. They work together for users to perform authentication and authorization functions in ITOC UI.

- **Authentication** - Configure and manage multiple LDAP identity servers for each organization (see Configure and Manage Authentication).
- **Groups** - Add groups to help manage what roles can be assigned to its users (see Add Groups and Associate Business Roles).
- **Business Roles** - Associate groups with roles or roles with groups, giving users permissions to view and access information in ITOC UI (see Add Groups and Associate Business Roles).

Note that the URL for the organization is automatically assigned and generated using server location information and the name of the organization to create the URL. Once generated, it is not editable.

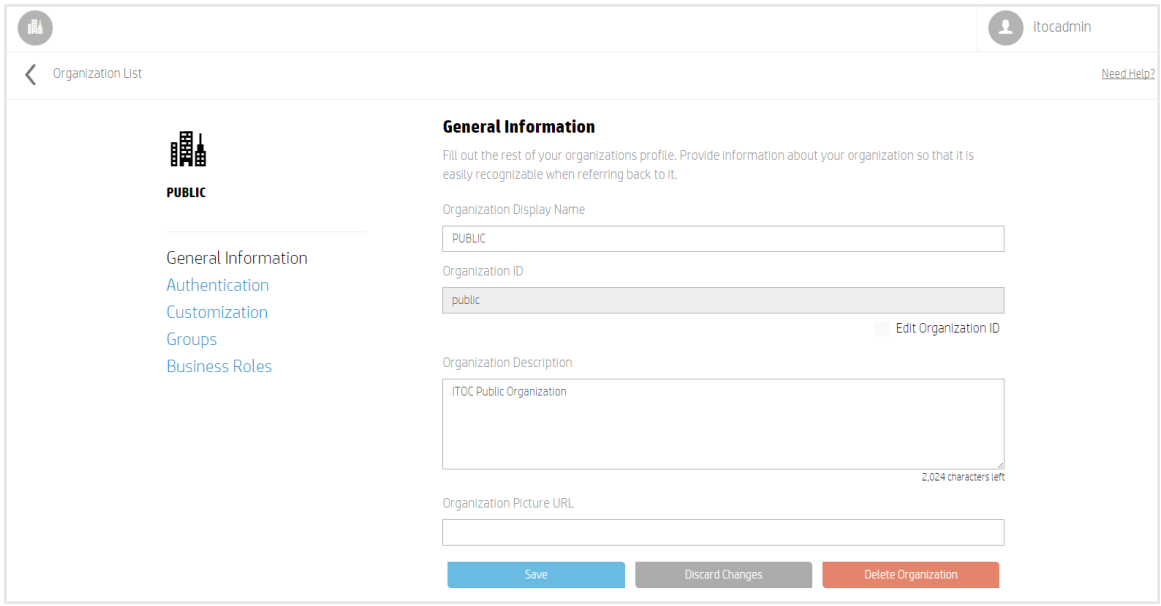
To create a new organization:

1. From your browser, log in to the **Organizations Administration UI** using port 9200. For example:

   `https://<ITOC_hostname>:9200`

2. The **Create and Manage Your Organizations** view opens, and the current organizations in the system are shown.
3. Click the **Add New Organization** widget.
4. In the **Create Organization** window, type in your new **Organization Name**. The system will create a unique **Organization ID** based on your Organization Name, which is a unique identifier in ITOC.
5. Press **Create**.
6. A dialog page appears, with the following five page links:
   - **General Information**
   - **Authentication**
   - **Customization**
   - **Groups**
   - **Business Roles**

7. Click the **General Information** view:



- Note that the **Organization Name** used to create the organization is now the **Organization Display Name**. In this view, you can edit your **Organization Display Name**:

    1. Enter a full description of your new organization.
    2. You can use a default image to represent the organization, or you can use the organization picture URL field to input an image from any live URL.
    3. Press the **Save** button.

    > **Note:** If you have if have not saved your last change while creating an organization, a screen called **Unsaved Changes** appears. This feature allows you to **Return to Page** where you can edit and save your most recent changes, or **Discard Changes** to proceed to the **Authentication** section.

- The **Organization ID** is grayed out, as it is uneditable by end users. This is the unique organization name used to identify your organization.

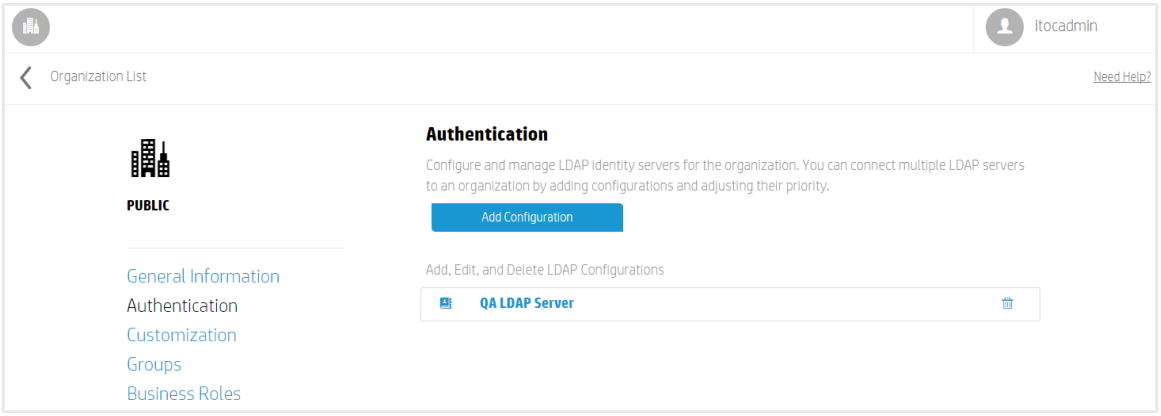
8. Click the **Authentication** tab, and enter your LDAP information. You will set your LDAP attributes and privileges for users, groups, and other basic authentication information for integration with your organization. For information on authentication and setting up LDAP, see Configure and Manage Authentication.
9. Click the **Customization** tab to customize the organization. For more information on

customizing organizations, see Create and Manage Organizations.

10. Press **Save**.

Configure and Manage Authentication

You can connect multiple LDAP servers by adding configurations and adjusting their relative priority within an organization.



LDAP is used to:

- Authenticate a user's login.
- Authenticate a user's access to information.
- Authorize a user's access to information.

To completely configure access to ITOC, you must configure LDAP to authenticate a user's login, configure LDAP for an organization to authenticate a user's access to information, and configure access control for an organization to authorize a user's access to information.

To configure LDAP for an organization:

1. Click the **Authentication** link.
2. To add a configuration, click the **Add Configuration** button.

   Or

   To edit a configuration, click on the display named of an existing LDAP.

   Add or edit the following information:

   LDAP Server Information

Item	Description
Display Name	The display name for the LDAP server.
Hostname	The fully qualified LDAP server domain name (`server.domain.com`) or IP address. Example: `ldap.xyz.com`
Port	The port used to connect to the LDAP server (by default, `389`). Example: `389`
SSL Connection	If the LDAP server is configured to require LDAPS (LDAP over SSL), select the **SSL Connection** checkbox.
Base DN	Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the basis of a search. Example: `o=xyz.com`
User ID (Full DN)	The fully distinguished name of any user with authentication rights to the LDAP server. If the LDAP server does not require a User ID or password for authentication, this value can be omitted. Example: `uid=admin@xyz.com,ou=People,o=xyz.com`
Password	Password of the User ID. If the LDAP server does not require a User ID or password for authentication, this value can be omitted.
Retype Password	Retype the password of the User ID.

LDAP Attributes

Enter the names of the attributes whose values are used for email notifications, authentication, and approvals in HP ITOC.

Item	Description
User Email	The name of the attribute of a user object that designates the email address of the user. The email address is used for notifications. If a value for this attribute does not exist for a user, the user does not receive email notifications.

Item	Description
	Default: `mail`
Group Membership	The name of the attribute(s) of a group object that identifies a user as belonging to the group. If multiple attributes convey group membership, the attribute names should be separated by a comma. Default: `member,uniqueMember`
Manager Identifier	The name of the attribute of a user object that identifies the manager of the user. Default: `manager`
Manager Identifier Value	The name of the attribute of a user object that describes the value of the Manager Identifier's attribute. For example, if the value of the Manager Identifier attribute is a distinguished name (such as `cn=John Smith`, `ou=People`, `o=xyz.com`) then the value of this field could be `dn`. Or, if the Manager Identifier is an email address (such as `admin@xyz.com`), then the value of this field could be `email`. Default: `dn`
User Avatar	LDAP attribute whose value is the URL to a user avatar image that will display for the logged in user portal. If no avatar is specified, a default avatar will be used.

User Login Settings

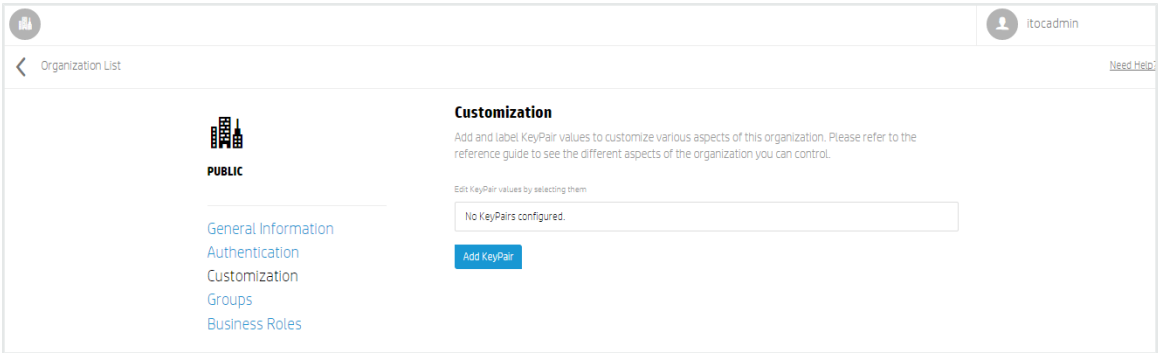
A user search-based login method is used to authenticate access to information.

Item	Description
User Name Attributes	The name of the attribute of a user object that contains the username that will be used to log in. The value for this field can be determined by looking at one or more user objects in the LDAP directory to determine which attribute consistently contains a unique user name. Often, you will want a **User Name Attribute** whose value in a user object is an email address. Examples: `userPrincipalName` or `sAMAccountName` or `uid`

Item	Description
User Search-base	The location in the LDAP directory where users' records are located. This location should be specified relative to the base DN. If users are not located in a common directory under the base DN, leave this field blank. Examples: `cn=Users` or `ou=People`
User Search Filter	Specifies the general form of the LDAP query used to identify users during login. It must include the pattern `{0}`, which represents the user name entered by the user when logging in. The filter is generally of the form `<attribute>= {0}`, with `<attribute>` typically corresponding to the value entered for **User Name Attribute**. Examples: `userPrincipalName={0}` or `sAMAccountName={0} or uid={0}`
Search Option (Search Sub-tree)	When a user logs in, the LDAP directory is queried to find the user's account. The **Search Subtree** setting controls the depth of the search under **User Search Base**. If you want to search for a matching user in the **User Search Base** and all subtrees under the **User Search Base**, make sure the **Search Subtree** checkbox is selected. If you want to restrict the search for a matching user to only the **User Search Base**, excluding any subtrees, unselect the **Search Subtree** checkbox.

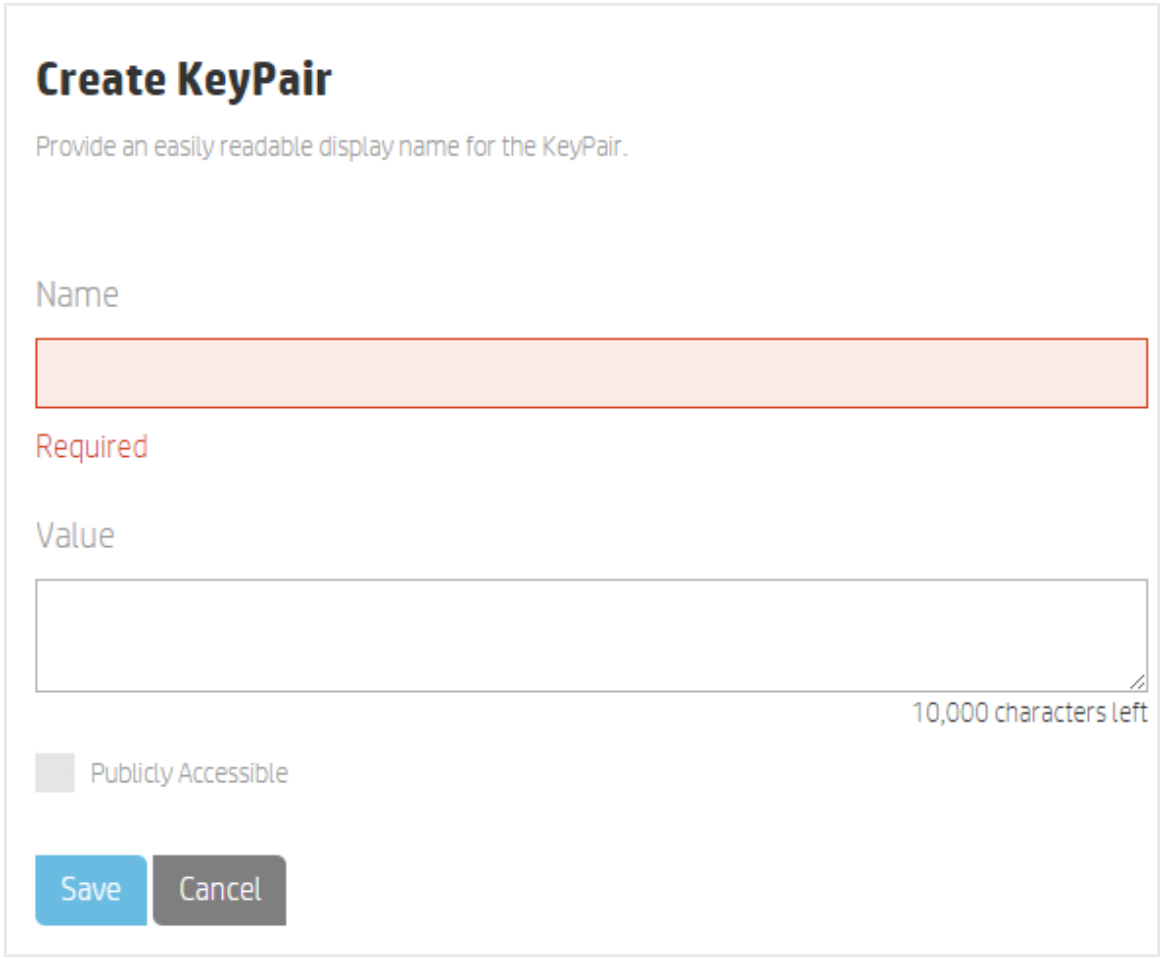
Customize a Consumer Organization

From the **Customization** screen, you can customize various aspects of a consumer organization by adding and labeling **KeyPair Values**.



To customize a consumer organization:

1. Click the **Customization** view.
2. Click **Add KeyPair**. The **Create KeyPair** dialog appears:



   - **Name** - Enter a required display name for the KeyPair.
   - **Value** - Enter a value for the KeyPair.
   - **Publicly Accessible** - Check the box to make the organization publicly accessible.
3. Press **Save**.

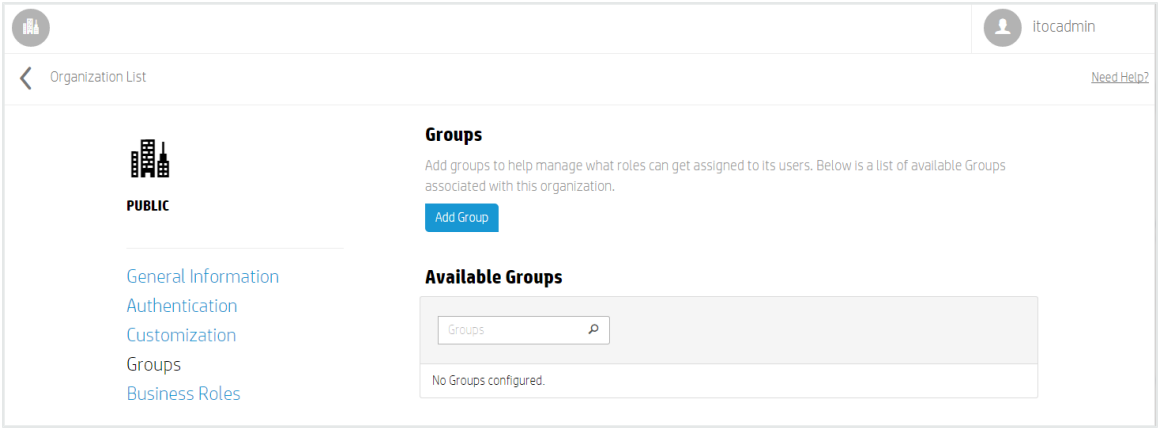
Application Labeling

KeyPair Value	Description
portalTitle	Type a name that displays on the login screen and header of your organization's portal.

KeyPair Value	Description
portalWelcomeMsg	Type a welcome message that displays below the Application Name when a user logs into your organization's portal.
portalFooterMsg	Type a footer message that displays below the login screen and header of your organization's portal.

Add Groups and Associate Business Roles

You can map LDAP groups in the organization administration, giving users in the LDAP groups login authentication on ITOC UI. The **Available Groups** list in this view shows groups associated with this organization:



To add a Group:

1. Click the **Groups** view.
2. Click the **Add Group** button.
3. Provide a **Group Name** and **Distinguished Name**. Both fields are required to create a group.
4. Press **Create**.

There are two ways to associate roles with the group:

1. From **Groups**, click the **Group** name link, which brings you to the **Groups** view.
2. Search for a role to associate with the group.
3. Select a role and click **Add Role**.
4. Click **Save** to make the association.

Or

1. After you create a group, go to the **Business Roles** link below **Groups**.
2. To associate a group with a role, click **Add Group** below the desired role.
3. Select a group to be associated with the chosen role from the dropdown list.
4. Click **Save** to make the association.

Validate that your group has a newly associated role:

1. Click on the group link for the group you want to view.
2. In the Groups view, you should see the new role association for your group listed in the **Associated Roles** section.

Repeat this process as needed to associate additional groups and roles in your organization.

Edit Groups

You can edit the group name and distinguished name of a group in the **Groups** view. Click on the group name link, make your name changes in the **Group Name** and **Distinguished Name** fields, then click the **Save** button.

Delete Associated Roles

There are two ways to delete an role association from a group:

1. In the **Groups** view, click on the link for the group. Under **Associated Roles**, click the '**X**' to the right of the role to delete this association, or:
2. In the **Business Roles** view, click the '**X**' to the right of the group to delete this association.
3. The following message appears: **No roles associated with this group**.

Remove Groups

1. Click on the **Groups** link to bring up the **Groups** view, click on the trashcan icon to the right of the **Group** name.
2. A warning window appears, allowing you to either **Remove Group** or **Cancel** the deletion.
3. Click **Remove Group**.

Disable Seeded Users

Once you have integrated with LDAP, you can disable ITOC seeded users:

1. Open the : `/opt/hp/itoc/wildfly-8.1.0.Final/standalone/deployments/idm-service.war/WEB-INF/classes/itoc-users.properties` file.
2. Remove all seeded user lines except `hpSysUser`.
3. Remove these lines :
   - `itocadmin=ENC(MY0BP7YrmM2U0ySCpJQsrlonVuxq2qbqUIJ0zsvbf+yJbaltebzI4CCDSjlMnOFNlPcqvbpw1UnjcgjXED7LweOyTfgRVl3tovMfLzMe8ZbUemePwE83+SUHLQgri/x7o6KT0pH7odamyLyhobWtha6SsgeLVf/4pwjxcU3oTRXtbAoVFolOWCswlWKZYG8DB7KgGwn/GwmJU4Ne3dFB7A==)`
   - `approver=ENC(iOZ6Rf8wu/W8F2hsvdy0qrEZL0p76cR2eC/CgJ//e/IRidU61Mc5IEI9Y4TQb6aWnDovmoI1SlhY Inf56BCPmAM+25Bn2mhrmA-joleeqi2HpkpLmvt6BUDC/LjXl5phe+V3wYRYspYOq8RMTe1FzlTd5jCcwMinQ)`
   - `serviceowner=ENC(DEWrnGaec/alFZMVF8t8zs6QPjQws7AJq6tulT9ltY1Gn4wzYN8jfr2GGdlaZlp/)`
   - `compliancearchitect=ENC(fgTANEAtGKT3JW62u7UwziWHCCJkWNduZFsTJEDYVpVfZ6DmwSYBwfel+E3N1bOI)`
   - `platformengineer=ENC(s/AUlhCdg601j00wUe/GK1MrwLJskumCTEnKZbtNA6siEcuxk3sGXg==`
   - `viewer=ENC(ujMQ/Uffn6Bb7lEI5+MYlMwgpkQpZF6BGhELOEK8aIc=)`
   - `jobrunner=ENC(N6zxNl54xjFy+oo5LBLnzWIn-pB4TLqAG49wyc2ftwRl3z4fyBnSWT8gF1LeapoVsTt3s9M/SS7C4lW6hIlFqY8K6erE2D`
4. Save the file.

   After seeded users are removed, they still can log in until after the first user data synchronization after removal occurs.

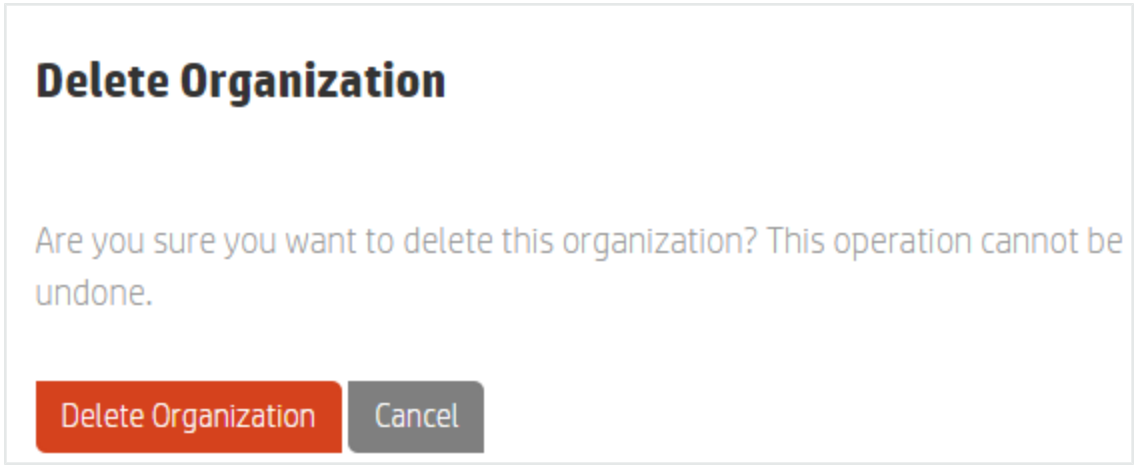
   Initial user data synchronization occurs 1 hour after ITOC startup and then every 12 hours by default. This value can be changed and used for subsequent user data synchronization occurrences.

Business Roles

From the **Business Roles** view, you can associate a group with a business role or delete an association from a role.

Delete an Organization

1. Click the **General Information** link.
2. Click the **Delete Organization** button. The following dialog appears:



3. Click the **Delete Organization** button.

Send Documentation Feedback

If you have comments about HP ITOC or this document, contact HP. If an email client is configured on this system, click the link above to generate an email to the HP ITOC team. Just add your feedback to the email and click send.

If no email client is available, send your feedback to itopscompliance@hp.com. Please include the name and version of the document in your feedback memo.

We appreciate your feedback!