



# IT Operations Compliance

Software Version: 1.20

Linux, Solaris, AIX, HP-UX, and Windows

## Administration Guide

Document Release Date: October 2016

Software Release Date: October 2016



**Hewlett Packard**  
Enterprise

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

© 2015 - 2016 Hewlett Packard Enterprise Development LP

### 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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

## Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** 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 HPE sales representative for details.

## Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

**HPE Software Solutions Now** accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

# Contents

View the administration UI in HPE ITOC .....	6
Users .....	8
View users in HPE ITOC .....	8
Roles and permissions .....	10
Roles .....	10
Permissions .....	13
HPE ITOC permissions .....	13
Notifications .....	16
Notification types .....	16
Subscribers .....	16
Notification types .....	17
Event-driven types .....	17
Reminder types .....	19
Compliance Status .....	20
View notifications .....	21
Edit notifications .....	22
Configure SMTP for notifications .....	23
Maintenance windows .....	24
Maintenance window work prioritization .....	24
View maintenance windows .....	25
Create a new maintenance window .....	25
Manage maintenance windows .....	28
View maintenance windows details .....	28
Maintenance windows - jobs .....	30
Maintenance windows - where used .....	31
Resource managers .....	33
View resource managers .....	33
Create a resource manager .....	34
Author and edit resource managers .....	34
Resource manager details .....	34

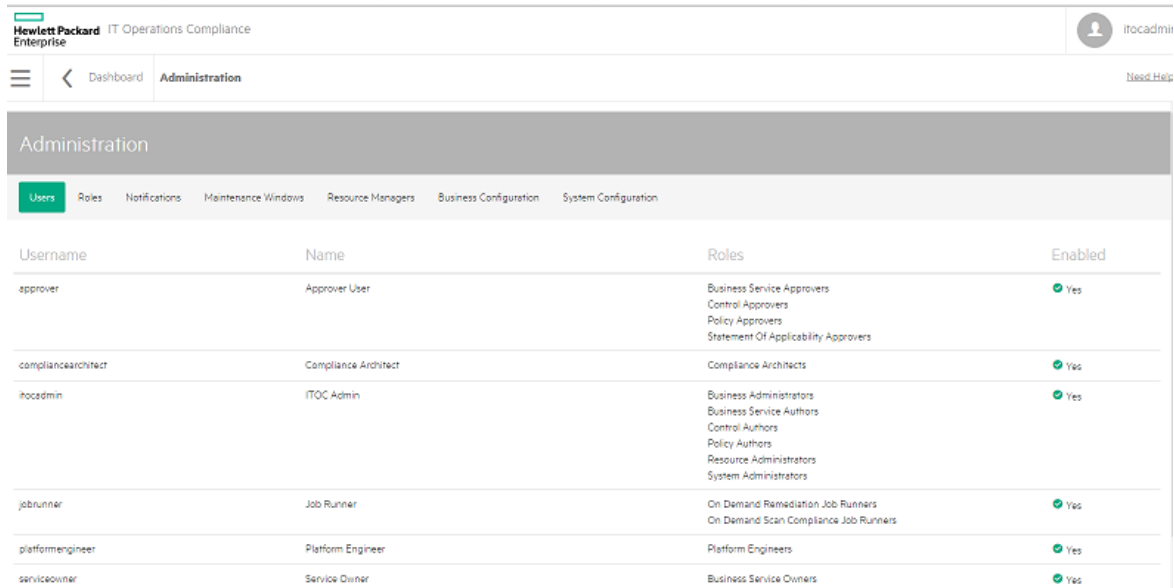
Resource manager history .....	35
<b>Business configuration .....</b>	<b>36</b>
Edit a business configuration .....	36
<b>System configuration .....</b>	<b>39</b>
<b>Organizations .....</b>	<b>42</b>
Public provider organizations .....	42
Consumer organizations .....	43
Log in to the Organizations Administration UI .....	43
Create and manage organizations .....	43
Create a new organization .....	44
Configure and manage authentication .....	46
Customize a consumer organization .....	50
Application labeling .....	50
Add groups and associate business roles .....	51
Add a group .....	51
Edit groups .....	52
Delete associated roles .....	52
Remove groups .....	52
Business roles .....	53
Delete an organization .....	53
Disable seeded users .....	53
<b>Send documentation feedback .....</b>	<b>55</b>

## View the administration UI in HPE ITOC

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

HPE ITOC has a separate Organizations Administration UI that the seeded itocadmin user can use to create organizations. For more information, see ["Organizations" on page 42](#).

To see the **Administration** UI, a user must belong to either the Business Administrators or the System Administrators role. A user belonging to the Maintenance Windows Managers role can see only the **Maintenance Windows** tab.



The screenshot shows the Administration UI for HPE ITOC. The top navigation bar includes the Hewlett Packard Enterprise logo, the text "IT Operations Compliance", and a user profile icon for "itocadmin". Below the navigation bar, there are tabs for "Users", "Roles", "Notifications", "Maintenance Windows", "Resource Managers", "Business Configuration", and "System Configuration". The "Users" tab is selected, displaying a table with the following data:

Username	Name	Roles	Enabled
approver	Approver User	Business Service Approvers Control Approvers Policy Approvers Statement Of Applicability Approvers	Yes
compliancearchitect	Compliance Architect	Compliance Architects	Yes
itocadmin	ITOC Admin	Business Administrators Business Service Authors Control Authors Policy Authors Resource Administrators System Administrators	Yes
jobrunner	Job Runner	On Demand Remediation Job Runners On Demand Scan Compliance Job Runners	Yes
platformengineer	Platform Engineer	Platform Engineers	Yes
serviceowner	Service Owner	Business Service Owners	Yes

- **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.
- **Resource Managers** - View, edit, and create resource managers
- **Business Configuration** - Editable and set as per organization

Users belonging to 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.

# Users

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

## View users in HPE ITOC

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

Username	Name	Roles	Enabled
approver	Approver User	Business Service Approvers Control Approvers Policy Approvers Statement Of Applicability Approvers	Yes
compliancearchitect	Compliance Architect	Compliance Architects	Yes
itocadmin	ITOC Admin	Business Administrators Business Service Authors Control Authors Policy Authors Resource Administrators System Administrators	Yes
jobrunner	Job Runner	On Demand Remediation Job Runners On Demand Scan Compliance Job Runners	Yes
platformengineer	Platform Engineer	Platform Engineers	Yes
serviceowner	Service Owner	Business Service Owners	Yes
viewer	Viewer User	Viewers	Yes

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

The following table lists all the seeded users in HPE ITOC.



- 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](#).

#### IHPE ITOCseeded users

User name	Name	Roles
<b>approver</b>	Approver User	<ul style="list-style-type: none"> <li>• Business services approvers</li> <li>• Control approvers</li> <li>• Policy approvers</li> <li>• Statement of applicability (SoA) approvers</li> </ul>
<b>compliancearchitect</b>	Compliance Architect	<ul style="list-style-type: none"> <li>• Compliance architects</li> </ul>
<b>csauser</b>	CSA User	<ul style="list-style-type: none"> <li>• Integration user</li> </ul>
<b>itocadmin</b>	ITOC Administrator	<ul style="list-style-type: none"> <li>• Business administrators</li> <li>• Business service authors</li> <li>• Control authors</li> <li>• CSA_ADMINISTRATION (visible only in the <b>Organizations Administration UI</b>)</li> <li>• Policy authors</li> <li>• Resource administrators</li> <li>• System administrators</li> </ul>
<b>jobrunner</b>	Job Runner	<ul style="list-style-type: none"> <li>• On-demand scan compliance job runners</li> <li>• On-demand remediation job runners</li> </ul>
<b>platformengineer</b>	Platform Engineer	<ul style="list-style-type: none"> <li>• Platform engineers</li> </ul>
<b>serviceowner</b>	Service Owner	<ul style="list-style-type: none"> <li>• Business service owners</li> </ul>
<b>viewer</b>	Viewer User	<ul style="list-style-type: none"> <li>• Viewers</li> </ul>

For information about integrating with LDAP and creating organizations and users, see [Organizations Overview](#).

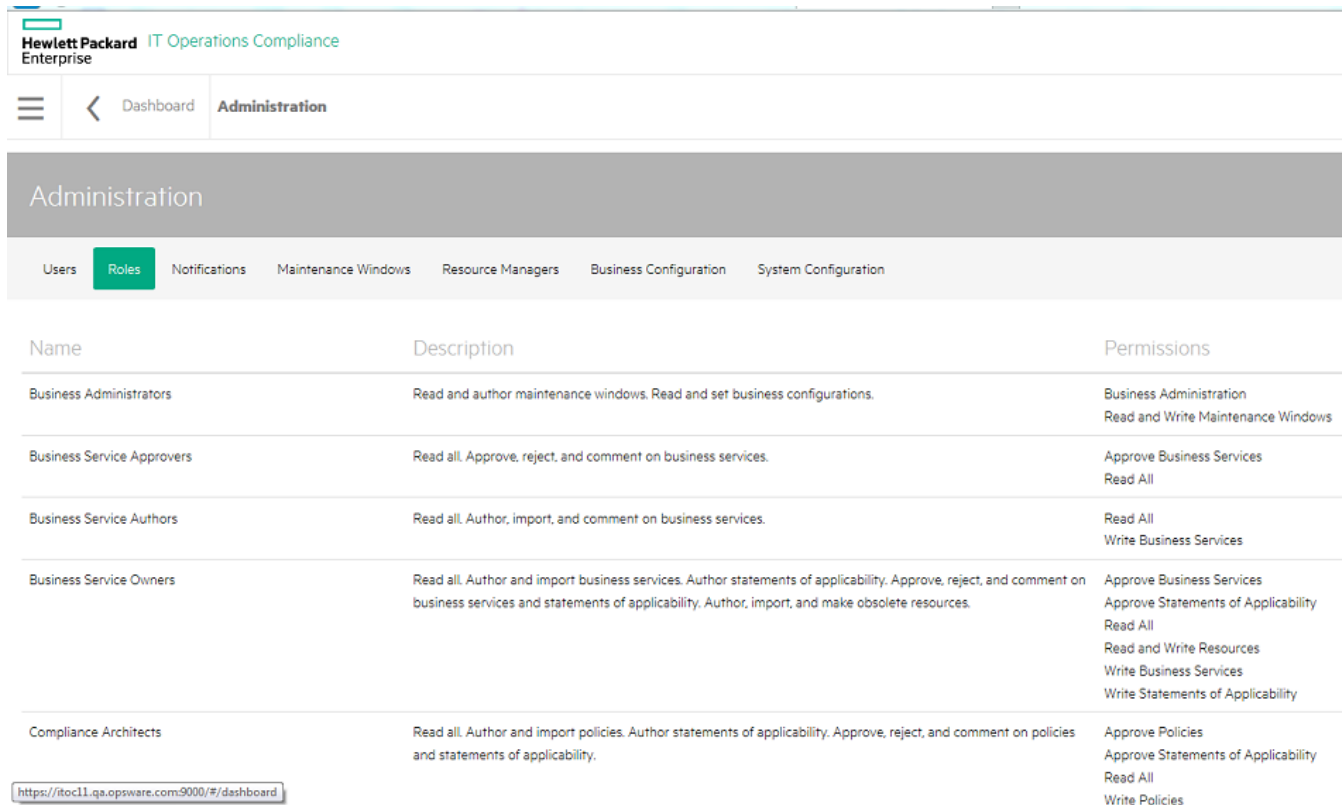
# Roles and permissions

This topic describes HPE ITOC roles and permissions.

- "Roles" below
- "Permissions" on page 13

## 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 policies and business service owners to manage business services and create SoAs. Roles cannot be added, edited, or deleted.



Name	Description	Permissions
Business Administrators	Read and author maintenance windows. Read and set business configurations.	Business Administration Read and Write Maintenance Windows
Business Service Approvers	Read all. Approve, reject, and comment on business services.	Approve Business Services Read All
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 statements of applicability. Approve, reject, and comment on business services and statements of applicability. Author, import, and make obsolete resources.	Approve Business Services Approve Statements of Applicability Read All Read and Write Resources Write Business Services Write Statements of Applicability
Compliance Architects	Read all. Author and import policies. Author statements of applicability. Approve, reject, and comment on policies and statements of applicability.	Approve Policies Approve Statements of Applicability Read All Write Policies

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

**ITOC roles and responsibilities**

Name	Description	Permissions
<b>Business Administrators</b>	<ul style="list-style-type: none"> <li>• Read and author maintenance windows.</li> <li>• Read and set business configurations.</li> </ul>	<ul style="list-style-type: none"> <li>• Business Administration</li> <li>• Read and Write Maintenance Windows</li> </ul>
<b>Business Service Approvers</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Approve, reject, and comment on business services.</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Business Services</li> <li>• Read All</li> </ul>
<b>Business Service Authors</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Author, import, and comment on business services.</li> </ul>	<ul style="list-style-type: none"> <li>• Read All</li> <li>• Write Business Services</li> </ul>
<b>Business Service Owners</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Author and import business services.</li> <li>• Author SoAs.</li> <li>• Approve, reject, and comment on business services and SoAs.</li> <li>• Author, import, and make obsolete resources.</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Business Services</li> <li>• Approve Statements of Applicability</li> <li>• Read All</li> <li>• Read and Write Resources</li> <li>• Write Business Services</li> <li>• Write Statements of Applicability</li> </ul>
<b>Compliance Architects</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Author and import policies.</li> <li>• Author SoAs.</li> <li>• Approve, reject, and comment on policies and SoAs.</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Policies</li> <li>• Approve Statements of Applicability</li> <li>• Read All</li> <li>• Write Policies</li> <li>• Write Statements of Applicability</li> </ul>
<b>Control Approvers</b>	<ul style="list-style-type: none"> <li>• Read controls.</li> <li>• Approve, reject, and comment on controls.</li> </ul>	<ul style="list-style-type: none"> <li>• Read and Approve Controls</li> </ul>
<b>Control Authors</b>	<ul style="list-style-type: none"> <li>• Read, author, import, and comment on controls.</li> </ul>	<ul style="list-style-type: none"> <li>• Read and Write Controls</li> </ul>
<b>Integration User</b>	<ul style="list-style-type: none"> <li>• Read and write access to</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Business Services</li> </ul>

Name	Description	Permissions
	all organizations.	<ul style="list-style-type: none"> <li>• Approve Statements of Applicability</li> <li>• Read All Organizations</li> <li>• Read All</li> <li>• Read and Write Maintenance Windows</li> <li>• Read and Write Resources</li> <li>• Read and Write All Organizations</li> <li>• Write Business Services</li> <li>• Write Statements of Applicability</li> </ul>
<b>Maintenance Window Managers</b>	<ul style="list-style-type: none"> <li>• Read and write maintenance windows.</li> </ul>	<ul style="list-style-type: none"> <li>• Read and Write Maintenance Windows</li> </ul>
<b>On Demand Remediation Job Runners</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Run on-demand remediation jobs.</li> </ul>	<ul style="list-style-type: none"> <li>• Read All</li> <li>• Run Remediation Jobs</li> </ul>
<b>On Demand Scan Compliance Job Runners</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Run on-demand scan compliance jobs.</li> </ul>	<ul style="list-style-type: none"> <li>• Read All</li> <li>• Run Scan Compliance Jobs</li> </ul>
<b>Platform Engineers</b>	<ul style="list-style-type: none"> <li>• Read, author, and import controls.</li> <li>• Approve, reject, and comment on controls.</li> </ul>	<ul style="list-style-type: none"> <li>• Read and Approve Controls</li> <li>• Read and Write Controls</li> </ul>
<b>Policy Approvers</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Approve, reject, and comment on policies.</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Policies</li> <li>• Read All</li> </ul>
<b>Policy Authors</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Author, import, and comment on policies.</li> </ul>	<ul style="list-style-type: none"> <li>• Read All</li> <li>• Write Policies</li> </ul>
<b>Resource Administrators</b>	<ul style="list-style-type: none"> <li>• Read, author, import, and make obsolete resources.</li> </ul>	<ul style="list-style-type: none"> <li>• Read and Write Resources</li> </ul>
<b>Statement of Applicability Approvers</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Approve, reject, and</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Statements of Applicability</li> </ul>

Name	Description	Permissions
	comment on SoAs.	<ul style="list-style-type: none"> <li>• Read All</li> </ul>
<b>Statement of Applicability Authors</b>	<ul style="list-style-type: none"> <li>• Read all.</li> <li>• Author, approve, reject, and comment on SoAs.</li> </ul>	<ul style="list-style-type: none"> <li>• Approve Statements of Applicability</li> <li>• Read All</li> <li>• Write Statements of Applicability</li> </ul>
<b>System Administrators</b>	<ul style="list-style-type: none"> <li>• Read and set system configurations.</li> </ul>	<ul style="list-style-type: none"> <li>• System Administration</li> </ul>
<b>Viewers</b>	<ul style="list-style-type: none"> <li>• Read all.</li> </ul>	<ul style="list-style-type: none"> <li>• Read All</li> </ul>

## 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.

### HPE ITOC permissions

Permission name	Permission description
<b>Approve Business Services</b>	<ul style="list-style-type: none"> <li>• Approves business services</li> <li>• Rejects business services</li> <li>• Comments on business services</li> <li>• Requires Read All permission</li> </ul>
<b>Approve Policies</b>	<ul style="list-style-type: none"> <li>• Approves policies</li> <li>• Rejects policies</li> <li>• Comments on policies</li> <li>• Requires Read All permission</li> </ul>
<b>Approve Statements of Applicability</b>	<ul style="list-style-type: none"> <li>• Approves SoAs</li> <li>• Rejects SoAs</li> <li>• Comments on SoAs</li> <li>• Requires Read All permission</li> </ul>
<b>Business</b>	<ul style="list-style-type: none"> <li>• Sets compliance threshold</li> </ul>

Permission name	Permission description
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Sets business object ID prefixes</li> <li>• Sets workflows</li> <li>• Configures notifications</li> </ul>
<b>Read All</b>	<ul style="list-style-type: none"> <li>• Views policy properties, requirements, rules, and compliance score</li> <li>• Views business service properties (including default maintenance windows), topology, and compliance score</li> <li>• Views SoA properties (including maintenance windows), exceptions, and compliance score</li> <li>• Views control properties and scripts</li> <li>• Views IT resource properties</li> <li>• Reads maintenance windows from the business service or SoA associated with a specified window</li> </ul>
<b>Read and Approve Controls</b>	<ul style="list-style-type: none"> <li>• Views control properties, scripts, and parameters</li> <li>• Approves on controls</li> <li>• Rejects on controls</li> <li>• Comments on controls</li> </ul>
<b>Read and Write Controls</b>	<ul style="list-style-type: none"> <li>• Views control properties, scripts, and parameters</li> <li>• Creates controls</li> <li>• Imports controls</li> <li>• Edits control properties, scripts, and parameters</li> <li>• Comments on controls</li> <li>• Submits controls</li> <li>• Makes controls obsolete</li> </ul>
<b>Read and Write Maintenance Windows</b>	<ul style="list-style-type: none"> <li>• Read maintenance windows</li> <li>• Create maintenance windows</li> <li>• Edit maintenance windows</li> <li>• Delete maintenance windows</li> </ul>
<b>Read and Write Resources</b>	<ul style="list-style-type: none"> <li>• Views resources and compliance score</li> <li>• Creates resources</li> <li>• Imports resources</li> <li>• Edits resources</li> <li>• Makes resources obsolete</li> </ul>

Permission name	Permission description
	<ul style="list-style-type: none"> <li>• Installs agents</li> </ul>
<b>Run Remediation Jobs</b>	<ul style="list-style-type: none"> <li>• Runs on-demand remediation jobs</li> <li>• Requires Read All permission</li> </ul>
<b>Run Scan Compliance Jobs</b>	<ul style="list-style-type: none"> <li>• Runs on-demand scan compliance jobs</li> <li>• Requires Read All permission.</li> </ul>
<b>System Administration</b>	<ul style="list-style-type: none"> <li>• Sets system configurations</li> <li>• Sets up email integration with SMTP</li> <li>• Sets schedule for recompliance calculation</li> <li>• Sets schedule for user to perform LDAP synchronization</li> </ul>
<b>Write Business Services</b>	<ul style="list-style-type: none"> <li>• Creates new business services or new draft revisions</li> <li>• Imports new business services</li> <li>• Edits business services properties and topology</li> <li>• Comments on business services</li> <li>• Submits business services</li> <li>• Makes business services obsolete</li> <li>• Requires Read All permission.</li> </ul>
<b>Write Policies</b>	<ul style="list-style-type: none"> <li>• Creates new policies or new draft revisions</li> <li>• Imports policies</li> <li>• Edits policy properties, requirements, and rules</li> <li>• Comments on policies</li> <li>• Submits policies</li> <li>• Makes policies obsolete</li> <li>• Requires Read All permission</li> </ul>
<b>Write Statements of Applicability</b>	<ul style="list-style-type: none"> <li>• Creates new SoAs and new draft revisions</li> <li>• Edits SoA properties and exceptions</li> <li>• Assigns maintenance windows to SoAs</li> <li>• Comments on SoAs</li> <li>• Submits SoAs</li> <li>• Makes SoAs obsolete</li> <li>• Requires Read All permission.</li> </ul>

# 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.

## Notification types

HPE 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. The **Notifications** view shows notifications by name and subscribers to each notification.

## 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 as follows:

- **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 the fixed [roles](#). If a role is selected, the notification is sent to all users who belong to that particular role.



# 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 Obsolete**

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.

**CSA Integration Completed**

When CSA integration is completed, a notification email is sent to Creator integration user.

**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.  
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.  
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 HPE 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 settings are set at a system level. For more information, see ["System configuration" on page 39](#).

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 MSLO 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 RSLO 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.

## 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 HPE ITOC system.

Name	Subscribers	Enabled
Object Revision Submitted for My Approval	Approver	Yes
Object Revision I Submitted was Rejected	Submitter	Yes
Object Revision Approved	Creator Submitter	Yes
Policy Revision Promoted to Production	Compliance Architects Business Service Owners Policy Authors Statement Of Applicability Authors	Yes
Business Service Revision Promoted to Production	Business Service Owners Business Service Authors Statement Of Applicability Authors	Yes
Statement of Applicability Revision Promoted to Production	Business Service Owners Statement Of Applicability Authors	Yes

- **Name** - Notification type.
- **Subscribers** - Roles of users who receive notifications (Creator, Submitter, Approver, Rejecter, Commenter).
- **Enabled** - Notifications are enabled by default.

## 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.

### Edit Notification

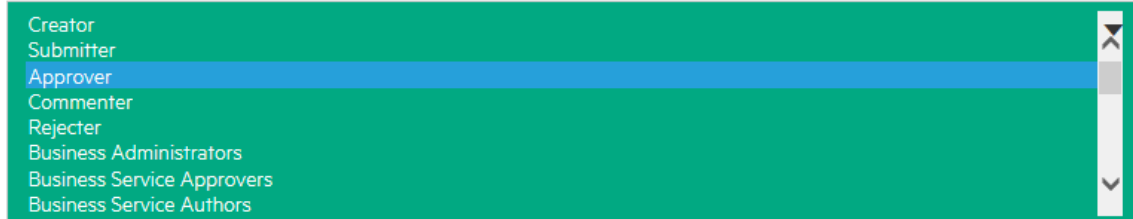
Name:

Object Revision Submitted for My Approval

Enabled

Subscribers:

Approver



OK

Cancel

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

## Configure SMTP for notifications

You must configure your SMTP server to send notifications. See ["System configuration" on page 39](#) for configuration details.

## Maintenance windows

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

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 time slot.

The HPE 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 (time slots) 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 time slot 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. One SoA may be assigned to multiple overlapping maintenance windows, which all may be run at the same time

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 time slot.

## View maintenance windows

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

The screenshot shows the Hewlett Packard Enterprise IT Operations Compliance Administration interface. The user is logged in as 'itocadmin'. The navigation menu includes 'Dashboard' and 'Administration'. The 'Administration' section is active, and the 'Maintenance Windows' tab is selected. The interface displays a table with the following data:

ID	Name	Window Type	
1	xx	Scan	✕
2	yy	Scan	✕

- **ID** - Maintenance window ID.
- **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 Maintenance Window**.



- **Name:** (required) 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)].  
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.  
**Note:** When you set the duration for an hourly job, the Start value must be 12:00 AM for the job to run hourly for 24 hours.
  - **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. Click **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.

## View maintenance windows details

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



☰ < Administration **Maintenance Window**

XX

Details Jobs Where Used

ID:	1
Window Type:	Scan
Window Start Time:	12:00 AM (UTC-08:00) Pacific Time (US & Canada)
Window End Time:	12:30 AM
Duration:	0.5 hours
Recurrence Type:	Daily
Window Start Date:	10/27/15
Created By:	on 10/27/15 10:18 AM
Modified By:	on 10/27/15 10:18 AM


### To edit maintenance windows properties...

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

A maintenance window cannot be modified while it is starting a new time slot; 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.

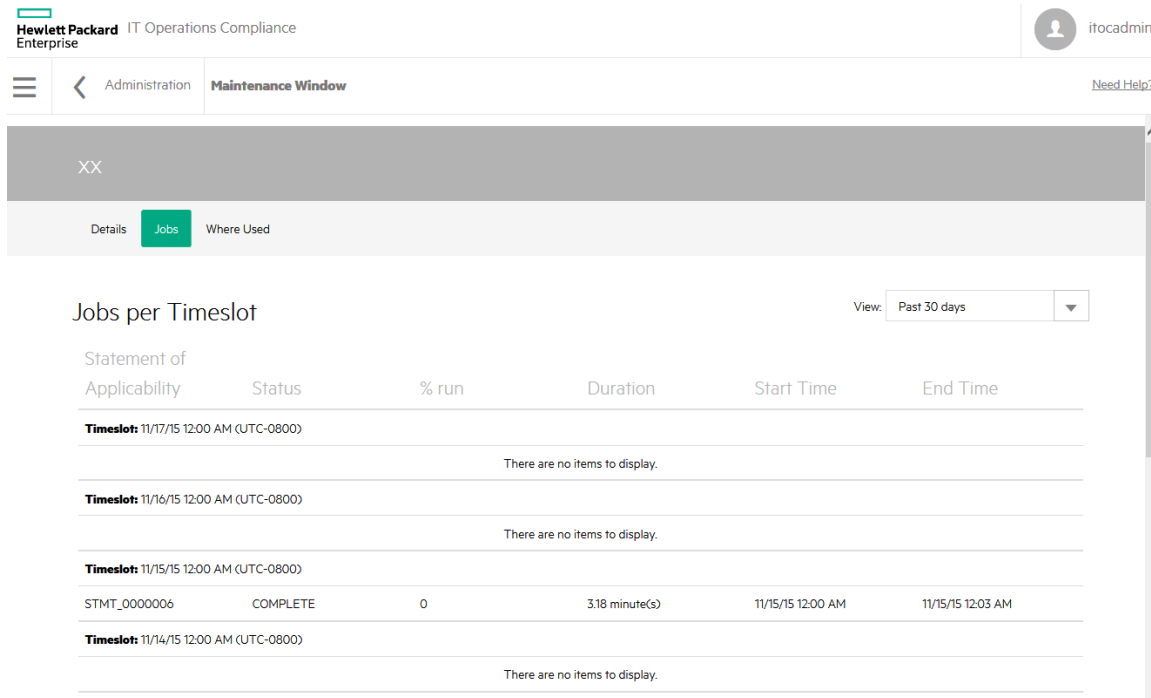
### To delete a maintenance window...

1. Click 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. Click the  icon in the row of the maintenance window you want to delete.
2. Click **OK** in the confirmation dialog that appears.

## Maintenance windows - jobs

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



Hewlett Packard Enterprise IT Operations Compliance

Administration Maintenance Window

itocadmin

Need Help?

XX

Details Jobs Where Used

Jobs per Timeslot View: Past 30 days

Statement of Applicability	Status	% run	Duration	Start Time	End Time
<b>Timeslot:</b> 11/17/15 12:00 AM (UTC-0800)					
There are no items to display.					
<b>Timeslot:</b> 11/16/15 12:00 AM (UTC-0800)					
There are no items to display.					
<b>Timeslot:</b> 11/15/15 12:00 AM (UTC-0800)					
STMT_0000006	COMPLETE	0	3.18 minute(s)	11/15/15 12:00 AM	11/15/15 12:03 AM
<b>Timeslot:</b> 11/14/15 12:00 AM (UTC-0800)					
There are no items to display.					

From **View:**, you can filter jobs per time slot 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 time slot.
- **Status** - Status of the job that was run during the specified maintenance window time slot:
  - **PENDING:** The maintenance window time slot has started and is planning work. Job is pending execution.
  - **IN PROGRESS:** The maintenance window time slot has started and is executing the job.
  - **COMPLETE:** The job has completed execution.
  - **INCOMPLETE:** The maintenance window time slot 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.

Jobs per Timeslot View: Past 30 days

Statement of Applicability	Status	% run	Duration	Start Time	End Time
<b>Timeslot:</b> 3/13/17 5:00 PM (UTC-0700)					
STMT_0000001	COMPLETE	100	0.81 minute(s)	3/13/17 6:00 PM	3/13/17 6:00 PM
<b>Timeslot:</b> 11/6/16 5:00 PM (UTC-0800)					
STMT_0000001	COMPLETE	100	0.95 minute(s)	11/6/16 5:00 PM	11/6/16 5:00 PM
<b>Timeslot:</b> 6/3/16 6:00 PM (UTC-0700)					
STMT_0000001	COMPLETE	100	0.81 minute(s)	6/3/16 6:00 PM	6/3/16 6:00 PM

**Scenario:**  
a) MW is UTC  
b) UI client in Pacific  
c) Job ran during Pacific Standard Time frame

**Scenario:**  
a) MW is UTC  
b) UI client in Pacific  
c) Job ran during Pacific Daylight Saving Time frame

## Maintenance windows - where used

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

Hewlett Packard Enterprise IT Operations Compliance itocadmin

Administration **Maintenance Window** Need Help?

XX

Details Jobs **Where Used**

Statements of Applicability Lifecycle: Active Statements

ID	Policy	Business Service	Measurement SLO	Remediation SLO	Revision
STMT_0000006	v4	b2	Within 1 Month	Comply within 14 days	2 (Production)

- **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

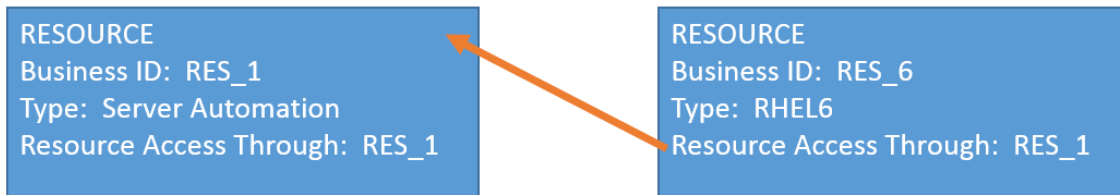


## Resource managers

Resources can be accessed through Resource Managers such as the HPE Server Automation (HPE SA) or HPE Cloud Service Automation (HPE CSA) core.

HPE ITOC supports integration with HPE SA. When used with HPE ITOC, HPE SA becomes a new resource manager, through which resources can be accessed.

The SA Resource Manager working with HPE ITOC allows users to install an agent on SA (along with a resource adapter). Users can create an HPE ITOC resource of type Server Automation (RES\_1 in the following figure) and have the HPE SA managed servers as HPE ITOC resources whose Resource Access Through property points to the Server Automation resource, RES\_1.



Each resource manager is an HPE ITOC Manager or Service Provider type.

## View resource managers

The **Resource Managers** view shows information about your resource managers. You can create and use HPE Cloud Service Automation and HPE Server Automation resource managers, through which you can access HPE ITOC resources.

The screenshot shows the HPE ITOC Administration interface. At the top left, it says 'Hewlett Packard Enterprise IT Operations Compliance'. On the top right, there is a user profile icon for 'itocadmin' and a 'Need Help?' link. Below the header, there is a navigation bar with 'Dashboard' and 'Administration' (selected). The main content area is titled 'Administration' and contains a menu with 'Users', 'Roles', 'Notifications', 'Maintenance Windows', 'Resource Managers' (highlighted in green), 'Business Configuration', 'System Configuration', and 'Actions' (with a dropdown arrow). Below the menu is a table with the following data:

ID	Name	Type	Status
RES_000006	sa mgr	HP Server Automation	Defined

From here, you can view:

- **ID** of the resource manager.
- **Name** of the resource manager.
- **Type** of resource manager (**Cloud Service Automation** or **Server Automation**).
- **Status** of the resource manager (**Defined**, **Managed**, or **Obsolete**).

## Create a resource manager

To create an SA or CSA resource manager, see the *HPE ITOC 1.20 Integration Guide*.

## Author and edit resource managers

"Resource manager details" below

"Resource manager history" on the next page

## Resource manager details

From the **Resource Managers** list, click the name of the resource manager whose details you want to view.

The screenshot shows the user interface for viewing resource manager details. At the top left is the Hewlett Packard Enterprise logo and the text "IT Operations Compliance". On the top right, the user "itocadmin" is logged in. Below the header, there are navigation tabs for "Administration" and "Resource", with "Resource" being the active tab. A "Need Help?" link is also present. The main content area has a grey header with a circular icon and the text "RES\_000006 - sa mgr". Below this, there are two tabs: "Details" (which is selected) and "History". To the right of these tabs is an "Actions" dropdown menu. The details section contains the following information:

Resource Type:	HP Server Automation
Description:	-
Version:	-
Host:	p
Port:	p
User:	p
Password:	<hidden>
Adapter Host:	p
Status:	Defined
Source URI:	
Source Ref:	sa_mgr_376d56cd-d2fa-4563-b404-71457f93aa74
Created By:	ITOC Admin on 10/27/15 11:42 AM
Modified By:	ITOC Admin on 10/27/15 11:42 AM

**To edit resource manager properties:**

1. Click **Actions** to select **Edit Properties**.
2. Modify the resource manager as needed.
3. Click **OK**.

## Resource manager history

The business service **History** view shows details about each revision's history, including:

- **Action** - What was done (created, submitted, and so on).
- **Notes** - Information provided by the user who created or modified the business service.
- **User** - Who performed the action.
- **Date** - Date and time the action was performed.

The screenshot shows the user interface for viewing the history of a resource manager. At the top, the Hewlett Packard Enterprise logo and 'IT Operations Compliance' are visible on the left, and the user 'itocadmin' is on the right. Below the navigation bar, the resource name 'RES\_000006 - sa mgr' is displayed. There are tabs for 'Details' and 'History', with 'History' being the active tab. An 'Actions' dropdown menu is also present. Below the tabs, the 'History' section contains a table with the following data:

Action	Notes	User	Date
Create	New Resource RES_000006 has been created.	ITOC Admin (itocadmin)	10/27/15 11:42 AM

**To view the history of a resource manager:**

1. Navigate to the **Resource Managers** tab, and click the resource whose history you want to view.
2. Click **History**.

## Business configuration

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

To view business configuration details:

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

The screenshot shows the Hewlett Packard Enterprise IT Operations Compliance Administration interface. The user is logged in as 'itocadmin'. The 'Administration' tab is selected, and the 'Business Configuration' sub-tab is active. The interface displays the following configuration details:

Administration									
Users	Roles	Notifications	Maintenance Windows	Resource Managers	<b>Business Configuration</b>	System Configuration	Workflow Providers	Actions	
Compliance									
Compliance Threshold:	100								
Vulnerability Threshold:	0.0								
Workflow									
Business Services:	Auto-Approval								
Controls:	Approval Required								
Policies:	Approval Required								
Statements of Applicability:	Approval Required								
Remediation Jobs:	Approval Required								
Business ID Prefix									
Business Services:	SVC_								
Controls:	CTRL_								
Policies:	POL_								
Resources:	RES_								
Statements of Applicability:	STMT_								

## Edit a business configuration

1. Click **Actions** and **Edit Business Configuration**. The **Edit Business Configuration** dialog appears.

**Edit Business Configuration**

Compliance:  
Compliance Threshold: 100

Workflow:  
Business Services: Auto-Approval

Controls: Approval Required

Policies: Auto-Approval

Statements of Applicability: Approval Required

Business ID Prefix:  
Business Services: SV  
Controls: CTRL  
Policies: POL  
Resources: RES  
Statements of Applicability: STMT

OK Cancel

2. In the **Compliance Threshold** field, enter the minimum percentage of compliance to be considered compliant overall. The value can be a number from 1 through 100. The default is 100.
3. Use the dropdown next to each entity to select the workflow for that entity. Workflow can be of the following types:
  - **Auto-Approval** - No approval is required. Submit takes the entity from draft to production.
  - **Approval Required** - The named approver must approve the entity before it can go into production.

The default workflow for each of the entities is:

- For Business Services: default is Auto-Approval
- For Controls: default is Approval Required
- For Policies: default is Approval Required
- For Statements of Applicability: default is Approval Required

4. In the **Business ID Prefix** section, 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.
5. Click **OK**.

Changes made apply to the organization to which the business administrator is logged in.

## 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.

The screenshot shows the Administration page of the Hewlett Packard Enterprise IT Operations Compliance system. The page has a header with the HP logo and the text "Hewlett Packard Enterprise IT Operations Compliance". Below the header is a navigation bar with a menu icon, a back arrow, and the text "Dashboard Administration". The main content area is titled "Administration" and contains a list of navigation links: "Users", "Roles", "Notifications", "Maintenance Windows", "Resource Managers", "Business Configuration", and "System Configuration". The "System Configuration" link is highlighted in green. Below the navigation links, there are three sections of configuration settings: "Tuning", "Notifications", and "LDAP".

Tuning	
Compliance Concurrency:	100
Log Level:	ERROR

Notifications	
Send Reminder N days before Event:	7
Send Reminder every N days after Event:	7
Send up to N Reminders after Event:	3
SMTP Host:	
SMTP Port:	25
SMTP User:	

LDAP	
User Data Synchronization Interval (hours):	12

To modify system configuration:

1. Click **Actions** and **Edit System Configuration**. The **Edit System Configuration** dialog appears.

## Edit System Configuration

---

### Tuning:

Compliance Concurrency:

100

Log Level:

ERROR

### Notifications:

Send Reminder N days before Event:

7

Send Reminder every N days after Event:

7

Send up to N Reminders after Event:

3

SMTP Host:

SMTP Port:

25

SMTP User:

SMTP Password:

Enter Password

Repeat Password

### LDAP:

User Data Synchronization Interval (hours):

12

OK

Cancel



## 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**.  
You must restart HPE ITOC after changing the log level for the new level to take effect.

## Notifications

- **Set Reminders N Days Before Event:** - The default is 7 (see "[Reminder types](#)" on page 19).
- **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 used 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

- **User Data Synchronization Interval (hours):** - How often LDAP synchronization is performed. The default is 12 hours.

2. Click **OK**.

# Organizations

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

An organization determines a user's entry point into the HPE ITOC system and associates its users with services and resources. The HPE 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.

HPE ITOC has two types of organizations:

- ["Public provider organizations" below](#) - The provider organization hosts HPE 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 HPELN 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" on the next page](#) - 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 HPE ITOC to access an LDAP server, at which point LDAP users can log into the HPE 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.
- Create one or more groups - Each group is a representation of an LDAP group.
- Assign roles to groups - Assigns roles to each group (see ["Roles" on page 10](#)).

## 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 in to the Organizations Administration UI

A user with the CSA\_ADMINISTRATION role can log in to the **Organizations Administration UI** using port 9200. For example:

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

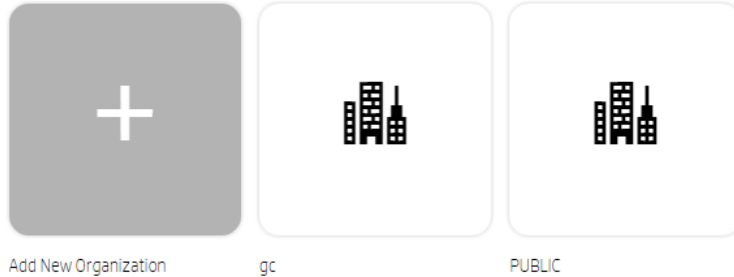
The **Create and Manage Your Organizations** view appears.

## Create and manage organizations

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



### Create and Manage Your Organizations



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" below](#) for more details.
- Navigate to an organization - Click the tile name of the organization to which you want to navigate.

## 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 the HPE ITOC UI.

- Authentication - Configure and manage multiple LDAP identity servers for each organization
- Groups - Add groups to help manage what roles can be assigned to its users (see ["Add groups and associate business roles" on page 51](#)).
- Business roles - Associate groups with roles or roles with groups, giving users permissions to view and access information in the HPE ITOC UI (see ["Add groups and associate business roles" on page 51](#)).

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 creates a unique organization ID based on your organization name, which is a unique identifier in HPE ITOC.
5. Click **Create**.
6. A dialog page appears, with the following 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.
    - i. Enter a full description of your new organization.
    - ii. 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.
    - iii. Click the **Save** button.

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.

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

**Org MNP**

General Information  
Authentication  
Customization  
Groups  
Business Roles

### General Information

Fill out the rest of your organizations profile. Provide information about your organization so that it is easily recognizable when referring back to it.

Organization Display Name  
PUBLIC

Organization ID  
org-mnp

Organization Description  
ITOC Public Organization  
2024 characters left

Organization Picture URL

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](#)" below
9. Click the **Customization** tab to customize the organization.
10. Click **Save**.

## Configure and manage authentication

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

## Authentication

Configure and manage LDAP identity servers for the organization. You can connect multiple LDAP servers to an organization by adding configurations and adjusting their priority.

Add Configuration

Add, Edit, and Delete LDAP Configurations

No LDAP servers configured.

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 HPE 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
<b>Display Name</b>	Display name for the LDAP server
<b>Hostname</b>	Fully qualified LDAP server domain name (server.domain.com) or IP address. Example: ldap.xyz.com
<b>Port</b>	Port used to connect to the LDAP server (by default, 389).

Item	Description
	Example: 389
<b>SSL Connection</b>	If the LDAP server is configured to require LDAPS (LDAP over SSL), select the <b>SSL Connection</b> check box.
<b>Base DN</b>	Base distinguished name. Base DN is the top level of the LDAP directory that is used as the basis of a search.  Example: o=xyz.com
<b>User ID (Full DN)</b>	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
<b>Password</b>	Password of the user ID. If the LDAP server does not require a user ID or password for authentication, this value can be omitted.
<b>Retype Password</b>	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 HPE ITOC.

Item	Description
<b>User Email</b>	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.  Default: mail
<b>Group Membership</b>	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
<b>Manager Identifier</b>	Name of the attribute of a user object that identifies the manager of the user.  Default: manager
<b>Manager</b>	Name of the attribute of a user object that describes the value of the



Item	Description
<b>Identifier Value</b>	<p>Manager Identifier's attribute. For example, if the value of the Manager Identifier attribute is a distinguished name (such as <code>cn=John Smith, ou=People, o=xyz.com</code>) then the value of this field could be <code>dn</code>. Or, if the Manager Identifier is an email address (such as <code>admin@xyz.com</code>), then the value of this field could be <code>email</code>.</p> <p>Default: <code>dn</code></p>
<b>User Avatar</b>	<p>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 is used.</p>

### User login settings

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

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

## Customize a consumer organization

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

The screenshot shows a user interface for customizing a consumer organization. At the top, there is a checkbox labeled 'Publicly Accessible'. Below this is a section titled 'themeName' with a text input field. To the right of the input field are two icons: a gear (settings) and a trash can (delete). Below the input field is another 'Publicly Accessible' checkbox. At the bottom of the form is a green button labeled 'Add KeyPair'.

To customize a consumer organization:

1. Click the **Customization** view.
2. Click **Add KeyPair**. The **Create KeyPair** dialog appears.
  - o **Name** - Enter a required display name for the KeyPair.
  - o **Value** - Enter a value for the KeyPair.
  - o **Publicly Accessible** - Check the box to make the organization publicly accessible.
3. Click **Save**.

## Application labeling

KeyPair Value	Description
<b>portalTitle</b>	Type a name that displays on the login screen and header of your organization's portal.
<b>portalWelcomeMsg</b>	Type a welcome message that displays below the application name when a user logs into your organization's portal.
<b>portalFooterMsg</b>	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 in the HPE ITOC UI. The **Available Groups** list in this view shows groups associated with this organization.

### Groups

Add groups to help manage what roles can get assigned to its users. Below is a list of available Groups associated with this organization.

Add Group

### Available Groups



No Groups configured.

## 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**.

## Business roles

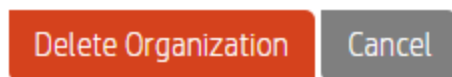
From the **Business Roles** view, you can associate a group with a business role or delete an association from a role.

## Delete an organization

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

### Delete Organization

Are you sure you want to delete this organization? This operation cannot be undone.



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

## Disable seeded users

Once you have integrated with LDAP, you can disable HPE 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  
(MY0BP7YrmM2U0ySCpJQsr1onVuxq2qbqUIJ0zsvbf+yJba1tebzI4CCDSj1Mn0FN1Pcqvpw1Unj  
cgjXED7Lwe0yTfgRV13tovMfLzMe8ZbUemePwE83+SUHLQgri/x7o6KT0pH7odamyLyhobWtha6S  
sgeLVf/4pwjxcU3oTRXtbAoVFo10WCswlWKZYG8DB7KgGwn/GwmJU4Ne3dFB7A==)
- approver=ENC  
(iOZ6Rf8wu/W8F2hsvdy0qrEZL0p76cR2eC/CgJ//e/IRidU61Mc5IEI9Y4TQb6aWnDovmoI1S1hY  
Inf56BCPmAM+25Bn2mhrmAjoleeqi2HpkpLmvt6BUDC/LjX15phe+V3wYRYspY0q8RMTe1Fz1Td5j  
CcwMinQ)
- serviceowner=ENC  
(DEWrnGaec/a1FZMVF8t8zs6QPjQws7AJq6tu1T91tY1Gn4wzYN8jfr2GGd1aZ1p/)
- compliancearchitect=ENC  
(fgTANEAtGKT3JW62u7UwziWHCCJKwNduZFstJEDYVpVfZ6DmwSYBwfe1+E3N1b0I)
- platformengineer=ENC(s/AUlhCdG601j00wUe/GK1MrwLJskumCTEnKZbtNA6siEcuxk3sGXg==
- viewer=ENC(ujMQ/Uffn6Bb71EI5+MY1MwgpkQpZF6BGhELOEK8aIc=)
- jobrunner=ENC  
(N6zxN154xjFy+oo5LbLnzWInpB4TLqAG49wyc2ftwR13z4fyBnSWT8gF1LeapoVsTt3s9M/SS7C4  
1W6hI1Fq  
Y8K6erE2DPwHtnq/A/00S15EXykUV8/BWjHRUuENw0ME)

4. Save the file.

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

# Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Administration Guide (IT Operations Compliance 1.20)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [hpe\\_itoc\\_docs@hpe.com](mailto:hpe_itoc_docs@hpe.com).

We appreciate your feedback!

