

VMware Workspace ONE Hub Services Documentation

APRIL 2024

VMware Workspace ONE

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

<https://docs.vmware.com/>

VMware by Broadcom

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2018-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. [Copyright and trademark information](#).

Contents

- 1 Setting Up Hub Services to Support Workspace ONE Intelligent Hub 6**
 - System Requirements for Hub Services 7
 - Administering Hub Services with Workspace ONE UEM and Workspace ONE Access 8
- 2 Activating Hub Services in VMware Workspace ONE Access 10**
 - How to Activate Hub Services with Workspace ONE UEM and Workspace ONE Access 11
 - Activate Hub Services for Existing Workspace ONE UEM Customers 12
- 3 Setting Up Hub Services for Your Organization 14**
 - Using Hub Services Without Enabling Workspace ONE Access 14
 - Using Hub Services When Workspace ONE Access Is Integrated 15
 - Using Hub Services When Workspace ONE UEM and Workspace ONE Access Are Integrated 16
 - Integrate Hub Services with Workspace ONE Intelligence to Share Hub Services Notification Analytics 17
- 4 Manage Admin Roles in Workspace ONE Hub Services 18**
 - Add Workspace ONE Access User Groups to Admin Roles in Hub Services 20
 - Adding Admin Groups and Assigning Customized Target Audience Permissions 22
- 5 Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users 26**
 - Managing Templates in Workspace ONE Hub Services 28
 - How to Add a Template in Workspace ONE Hub Services and Assign It to Groups 29
 - Configuring Templates to Restrict Access to Workspace ONE Intelligent Hub Features when Workers are Off Shift 33
 - Adding an Onboarding Template and Preparing the Welcome Page for Pre-Hires in Hub Services (Cloud Only) 35
- 6 Customizing the Workspace ONE Intelligent Hub App Layout 37**
 - Adding a Custom Tab to Workspace ONE Intelligent Hub 37
 - How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom Tab on the Web Portal 39
 - Customize Branding for the Workspace ONE Intelligent Hub App and Hub Portal 40
 - View Virtual Apps in Workspace ONE Intelligent Hub on Small Screens 45
 - Manage Launch Screens that Display in Workspace ONE Intelligent Hub 45
- 7 Setting up the Workspace ONE Intelligent Hub App Catalog in Hub Services 46**
 - Customize the Workspace ONE Intelligent Hub App Catalog in Hub Services 47
 - Add a Promotions Section to the Catalog App View in Workspace ONE Intelligent Hub 49

- Add Featured Categories as Sections in the Catalog View 49
- Setting Up Quick Actions in App Catalog Tab (Cloud only) 50
- Managing Desktops and Apps That Display in the Workspace ONE Intelligent Hub App Catalog 54
- Create a Pre-Hire Version of the Hub Catalog for Workspace ONE Intelligent Hub 56
- Migrating Workspace ONE UEM App Catalog Settings to Hub Services 57

- 8 Using Hub Notifications Service in Workspace ONE Hub Services 60**
 - Types of Notifications That Can Be Sent from Workspace ONE Hub Services 61
 - Creating Custom Notifications in Workspace ONE Hub Services 63
 - Change the Branding of Notifications Sent from Workspace ONE Hub Services 68
 - How Hub Services Notifications Display on User Devices 68
 - Create Notifications in Workspace ONE Hub Services 69
 - Example of How to Create Notifications in Workspace ONE Hub Services That Require Action 73
 - Example of How to Create an Informational Notification in Workspace ONE Hub Services 77
 - Action Methods That You Can Configure in the Workspace ONE Notifications API 78
 - Archiving Notifications (Cloud only) 78
 - Creating Notification Templates in Workspace ONE Hub Services 80
 - Setting Up Push Notifications in Hub Services for Workspace ONE Access (On Premises only) 83
 - Integrate Hub Services with Workspace ONE Intelligence to Provide Notification Analytics and Automation Workflows 84

- 9 Enabling Access to People Search in the Workspace ONE Intelligent Hub App 86**
 - Enable People Service in Hub Services 87

- 10 Configuring Workspace ONE Intelligent Hub Employee Self-Service Features in Hub Services 89**
 - Setting Up Self-Service Quick Actions in the Support Tab (Cloud only) 92

- 11 Using Hub Services Shift-Based Access Control to Manage Shift-Based Workers Access to Resources in Workspace ONE Intelligent Hub App 98**

- 12 About MDM Enrollment in Workspace ONE Intelligent Hub 99**
 - Workspace ONE Intelligent Hub App Mobile Device Management Settings 99
 - Enable Intelligent Hub Device Enrollment and Authentication Mode 101
 - Enable Unmanaged Enrollment for iOS Devices 102
 - Configure Contact Email and Phone Number Information for Workspace ONE Intelligent Hub Support Tab 103
 - Workspace ONE UEM Device Management Options for Public and Internal Apps 103
 - Managing Access to Applications in Workspace ONE UEM 105

	Configuring Mobile Single Sign-On from Workspace ONE UEM Enrolled Devices	105
	Set Up Workspace ONE UEM Enterprise Mobility Management on Google for Android	106
13	Deep Links to Workspace ONE Intelligent Hub Pages Supported on iOS and Android Devices	108
14	Deploying Workspace ONE Intelligent Hub App	110
	Distributing the Workspace ONE Intelligent Hub Application for iOS and Android	110
	Workspace ONE UEM Application Configuration for Enterprise Key Value Pairs	111
	Deploying Workspace ONE Intelligent Hub App for macOS	113
	How to Access the Intelligent Hub Portal from Web Browsers	114
15	User Experience in the Workspace ONE Intelligent Hub App	115
	Installing and Setting Up Workspace ONE Intelligent Hub App on Devices	116
	Setting Passcodes Before Accessing the Workspace ONE Intelligent Hub App	116
	User Experience When Accessing Apps from the Workspace ONE Intelligent Hub App	117
	Workspace ONE Intelligent Hub App Account Settings	118
	Using People Functionality in the Workspace ONE Intelligent Hub App	119
	Receiving Notifications in the Workspace ONE Intelligent Hub App	119
	Accessing Native Apps in Workspace ONE Intelligent Hub	122
	User Experience When Accessing Workspace ONE Intelligent Hub Portal in a Web Browser	122
	Account Settings Available in the Workspace ONE Intelligent Hub Web Browser View	123
16	Frequently Asked Questions about the VMware Workspace ONE Intelligent Hub App	125
17	Accessing Other Documents	134

Setting Up Hub Services to Support Workspace ONE Intelligent Hub

1

Hub Services is a service co-located with VMware Workspace ONE[®] Access[™] that lets you design and set up how employees use the VMware Workspace ONE[®] Intelligent Hub app to access, discover, and connect with corporate resources, teams, and workflows within a company. Users use the Workspace ONE Intelligent Hub app on devices or the Hub portal in a web browser to access the employee engagement features.

The table shows the features available for cloud and on-premises deployments.

Table 1-1. Hub Features for Workspace Cloud and Workspace ONE Access on-Premises Deployments

Hub Feature	Availability for Cloud Deployments	Availability for Workspace ONE Access On-Premises Deployments
App Catalog, known as Hub Catalog	Yes	Yes
Notifications	Yes	Yes
People	Yes	Yes
Employee Self-Service Support	Yes	Yes
Custom Tab	Yes	Yes
Branding	Yes	Yes
Shift-Based Access Control	Yes	No
Templates	Yes	Yes

You can use Hub Services templates to customize the Workspace ONE Intelligent Hub features for different groups of users based on their role, location, or other criteria. The groups you select to access the template can be Workspace ONE UEM smart groups or Workspace ONE Access groups. See [Chapter 5 Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users](#) .

When you use Hub Services with Workspace ONE UEM, without Workspace ONE Access, you can configure an app catalog in Hub Services to access UEM and web apps from the Workspace ONE Intelligent Hub app on user devices. You can also send out device notifications and set up an employee self-service page where employees can manage their devices and access help links that you define. You can customize the layout of the Workspace ONE Intelligent Hub app with branding changes, a custom tab, and your logo.

When Hub Services is configured with Workspace ONE Access without Workspace ONE UEM, users can access the app catalog through the Hub portal from a browser. You can set up the Hub portal so that users can access resources, receive notifications, and use the employee self-services page to access help links that you define. You can customize the layout of the portal with branding changes and your logo.

Read the following topics next:

- [System Requirements for Hub Services](#)
- [Administering Hub Services with Workspace ONE UEM and Workspace ONE Access](#)

System Requirements for Hub Services

To deploy Hub Services features, ensure that your VMware Workspace ONE UEM and VMware Workspace ONE Access deployments meet the necessary requirements.

Network Port Requirement for On Premise Workspace ONE Access Deployments

Source Component	Destination Component	Protocol	Port	Description
Workspace ONE Access host name	signing.awmdm.com	HTTPS	443	Mandatory to launch Hub Services console and to provision certificates for Workspace ONE Notifications service.

Workspace ONE Requirements

To use all the Hub Services features, make sure that you are using the latest versions of Workspace ONE UEM, Workspace ONE Access, and Workspace ONE Intelligent Hub app.

Web Browsers Supported for Hub Console and End User Access

- Google Chrome. The latest two versions.
- Mozilla Firefox. The latest version.
- Safari. The latest two versions.
- Microsoft Edge. The latest version.

Device Versions Supported

- iOS devices 11.0 or later.

- Android devices 7.X .X or later.
- Windows 11 and Windows 10 devices.
- macOS 10.12 or later.

Intelligent Hub App Versions

To use all the Hub Services features that are released and to ensure users operate in the most secure environments possible, make sure users update their devices to the latest version of the Workspace ONE Intelligent Hub app. See [KB 81271 VMware Workspace ONE Applications Policy](#).

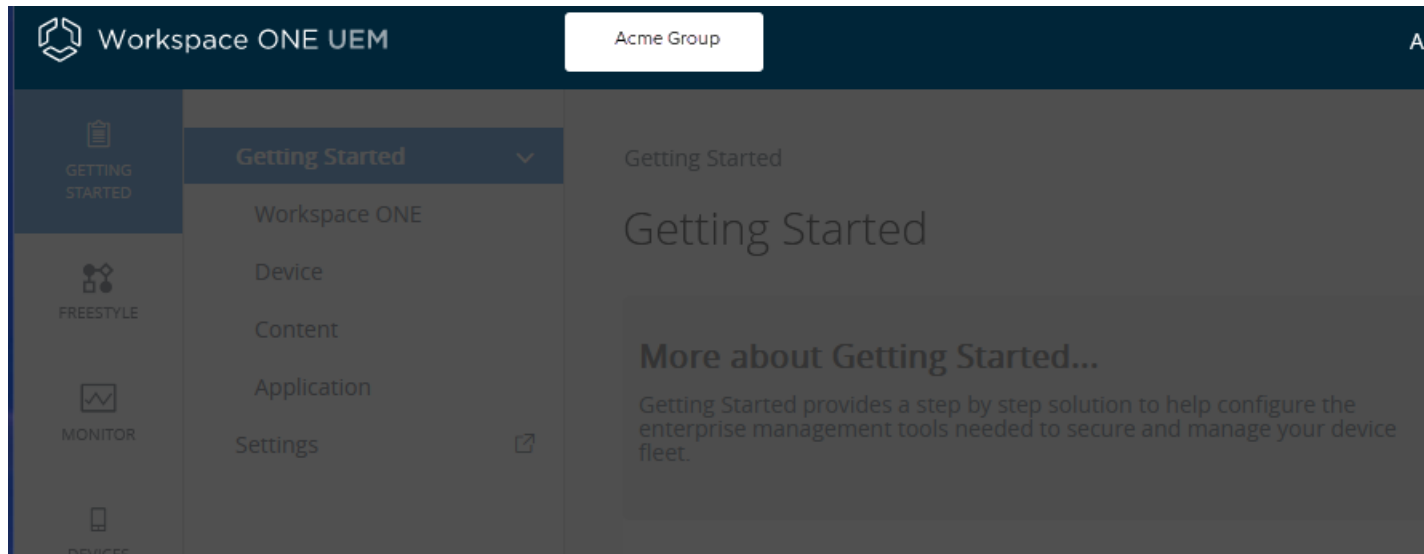
Administering Hub Services with Workspace ONE UEM and Workspace ONE Access

To configure and manage your Hub Services experience, you navigate between the different administration consoles.

- Workspace ONE Hub Services
- Workspace ONE Access
- Workspace ONE UEM

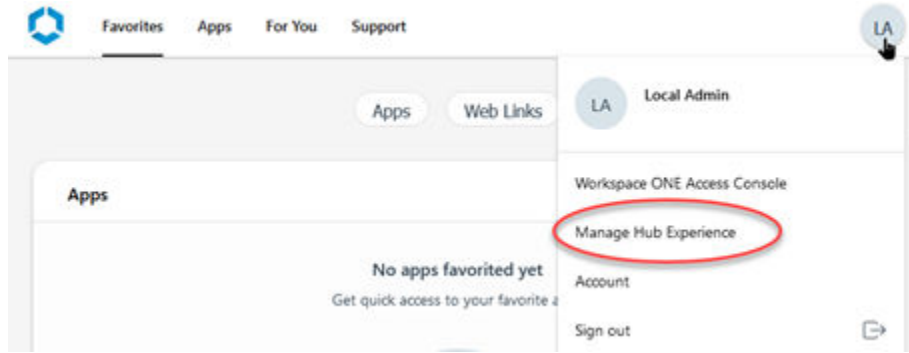
You can quickly switch between consoles from the UEM console. In the Workspace ONE UEM console, click the 3x3 icon in the right corner to switch between consoles.

Figure 1-1. Switching Between Different Consoles from the Workspace ONE UEM Console



You can access the Hub Services console from your Workspace ONE Intelligent Hub portal.

Figure 1-2. Access Hub Services Console from your Portal



For detailed information about configuring the services, see the appropriate documentation libraries. See [Chapter 17 Accessing Other Documents](#). The Using and Managing Hub Services guide is not meant to describe how to configure and manage Workspace ONE UEM and Workspace ONE Access.

Table 1-2. Major Intelligent Hub Tasks Performed from Each Administration Service

Workspace ONE UEM	Workspace ONE Access	Hub Services
<ul style="list-style-type: none"> ■ Run the Workspace ONE Getting Started Wizard to configure integration with Workspace ONE Access ■ Activate Hub Services to enable Hub Services features. ■ Set up device enrollment and management rules for devices that use single sign-on to the Workspace ONE Intelligent Hub app. ■ Create and manage UEM user accounts that access Hub Services features. This includes enabling the Local Basic User accounts for Workspace ONE. 	<ul style="list-style-type: none"> ■ Manage changes in the Workspace ONE UEM Integration page configured to create the trusted relationship with Workspace ONE UEM. ■ Configure authentication methods used for single sign-on. ■ Create conditional access policies to control access to resources. ■ Enable the compliance check feature to verify that managed devices adhere to Workspace ONE UEM compliance policies. ■ Map Identity Manager Domains to Customer Organization Groups in Workspace ONE UEM. 	<p>Manage the Hub Services features.</p> <ul style="list-style-type: none"> ■ App Catalog. Customize how apps displays in the app catalog and enable the app rating feature. Review the rating reports. ■ Enable the Custom tab and configure the URL. ■ Create templates to customize the Intelligent Hub experience for different users. ■ Enable People when UEM is integrated with Workspace ONE Access. ■ Create and send Notifications. ■ Manage Help and Support page content. ■ Manage the Hub Services system settings. ■ Customize branding.

Activating Hub Services in VMware Workspace ONE Access

2

The Hub Services component of Workspace ONE is co-located with Workspace ONE Access. To enable Hub Services functionality within the Workspace ONE Intelligent Hub app, Hub Services must be activated.

Hub Services can operate with Workspace ONE UEM alone providing a subset of Hub Services features - Catalog for UEM apps, Notification, Self-Service Support, and Custom Tab.

The full workspace experience with a unified catalog, engagement features like people search, enhanced notifications, and a web browser interface can be enabled when Workspace ONE Access is integrated with Workspace ONE UEM deployments.

Hub Services can operate with Workspace ONE Access on-premises deployments to provide the Hub Services features, Catalog, Notification, People, Self-Service Support, Custom Tab capabilities and Templates. When Workspace ONE UEM is integrated with on-premises deployments, users can use the Workspace ONE Intelligent Hub app to access their workspace on devices.

Workspace ONE Intelligent Hub Feature Capabilities

Hub Feature	Available with Workspace ONE UEM	Available with Workspace ONE Access
Templates	Yes	Yes
App catalog	Yes For Workspace ONE UEM apps	Yes Unified app catalog with SSO and conditional access
Customize Branding	Yes	Yes
Notifications Basic corporate communication	Yes	Yes
Notifications Workspace ONE Access must be integrated with Workspace ONE UEM.	No	Yes
Custom Tab	Yes	Yes
Employee Self-Service Support	Yes	Yes
People	No	Yes

Read the following topics next:

- [How to Activate Hub Services with Workspace ONE UEM and Workspace ONE Access](#)
- [Activate Hub Services for Existing Workspace ONE UEM Customers](#)

How to Activate Hub Services with Workspace ONE UEM and Workspace ONE Access

The activation flow for Hub Services depends on whether you are a new customer or an existing customer.

New Customers to Workspace ONE

Hub Services is activated automatically as part of the Workspace ONE instance provisioning process for new customers. Workspace ONE UEM, Workspace ONE Access, and Hub Services consoles are connected together, and the Hub catalog is enabled for the Workspace ONE Intelligent Hub app.

In the Hub Services console, you set up Hub Services for your organization and enable Hub Services functionality within the Workspace ONE Intelligent Hub app.

Existing Cloud Workspace ONE UEM Customers

If you are an existing Workspace ONE UEM customer, you received an email that includes a link to your Workspace ONE Access cloud tenant. If you did not access your Workspace One Access cloud tenant in a timely manner, your access link might have expired. To reactivate your tenant account or to retrieve your tenant URL, admin name, and password, contact either your Workspace ONE Support team or your account administrator. After you receive the tenant information, you can activate your Hub Services account in the Workspace ONE UEM console. See [Activate Hub Services for Existing Workspace ONE UEM Customers](#).

After Hub Services is activated, your next step is to go to the Hub Services console to configure the catalog view, add your logo and company branding colors, and enable other functionality.

Make sure that the Hub catalog is enabled and the correct authentication methods are configured. See [Chapter 7 Setting up the Workspace ONE Intelligent Hub App Catalog in Hub Services](#).

Existing and New Workspace ONE Access Customers

Customers who are using Workspace ONE Access in the cloud or as an on-premises deployment can use Hub Services capabilities in a web browser without integrating with Workspace ONE UEM. No additional setup is required. Go to the Hub Services console from the Workspace ONE Access console, Integrations > Hub Configuration page to launch Hub Services to access the Hub Services console. You can add your logo and company branding and enable other Hub Services functionality.

To use Hub Services capabilities with the Workspace ONE Intelligent Hub app, Workspace ONE Access must integrate with Workspace ONE UEM. See [Chapter 3 Setting Up Hub Services for Your Organization](#).

Activate Hub Services for Existing Workspace ONE UEM Customers

Because the Hub Services service is co-located with Workspace ONE Access, existing Workspace ONE UEM customers who want to use Hub Services must enter their Workspace ONE Access cloud tenant URL and OAuth 2.0 client ID and secret in the Workspace ONE UEM console to activate Hub Services.

If you do not have a Workspace ONE Access cloud tenant, contact your Workspace ONE support team or account administrator to request the tenant URL.

Prerequisites

In your Workspace ONE Access console, generate the Workspace ONE Access OAuth 2.0 service client with the client ID and shared secret. You configure the Workspace ONE Access tenant URL, client ID, and secret in the Workspace ONE UEM console. See the [Creating a Workspace ONE Access OAuth 2.0 Service Client for Workspace ONE UEM](#) article in the Workspace ONE Access Administration guide.

Procedure

- 1 In the Workspace ONE UEM console Groups & Settings page, select **Configurations > Intelligent Hub** click **Get Started**.
- 2 In the Activate Hub Services page, enter the Workspace ONE Access cloud tenant URL as **https://myco.vmware.com**. Enter the OAuth 2.0 service client ID and secret that you generated in the Workspace ONE Access console.
- 3 Click **TEST CONNECTION** to confirm that Workspace ONE UEM and Workspace ONE Access are communicating securely.

If the connection fails, check that the tenant URL and OAuth 2.0 client ID and secret values that you entered are the same as the OAuth 2.0 service client generated in the Workspace ONE Access console.

- 4 Click **Save**.

Results

Hub Services is activated, Workspace ONE Access and Workspace ONE UEM are linked together. The Intelligent Hub page is updated to show the Hub Services URL. You can now launch the Hub Services console from this page.

What to do next

Go to the Hub Services console and configure the Hub services for your organization and Hub Services functionality within the Workspace ONE Intelligent Hub app. See [Chapter 3 Setting Up Hub Services for Your Organization](#).

Setting Up Hub Services for Your Organization

3

The Workspace ONE Hub Services component is co-located with Workspace ONE Access and is dependent on Workspace ONE Access for shared services. When configured with Workspace ONE UEM, the Hub Services catalog for UEM apps, notifications from UEM, and a custom tab can be enabled for the Workspace ONE Intelligent Hub app on devices.

The Workspace ONE Intelligent Hub app facilitates MDM enrollment in the traditional MDM uses cases for Workspace ONE UEM deployments. You configure the MDM settings from the Workspace ONE UEM console [Device & Users > <Devicetype> Intelligent Hub Settings](#) page. See [Chapter 12 About MDM Enrollment in Workspace ONE Intelligent Hub](#).

The Workspace ONE Intelligent Hub app is installed on iOS, Android, macOS, and Windows devices to enroll the device and manage user access to their apps. By default, the Workspace ONE Intelligent Hub app runs in device management mode. When users initially launch the Workspace ONE Intelligent Hub app, they enter their corporate credentials to self-activate their devices.

Read the following topics next:

- [Using Hub Services Without Enabling Workspace ONE Access](#)
- [Using Hub Services When Workspace ONE Access Is Integrated](#)
- [Integrate Hub Services with Workspace ONE Intelligence to Share Hub Services Notification Analytics](#)

Using Hub Services Without Enabling Workspace ONE Access

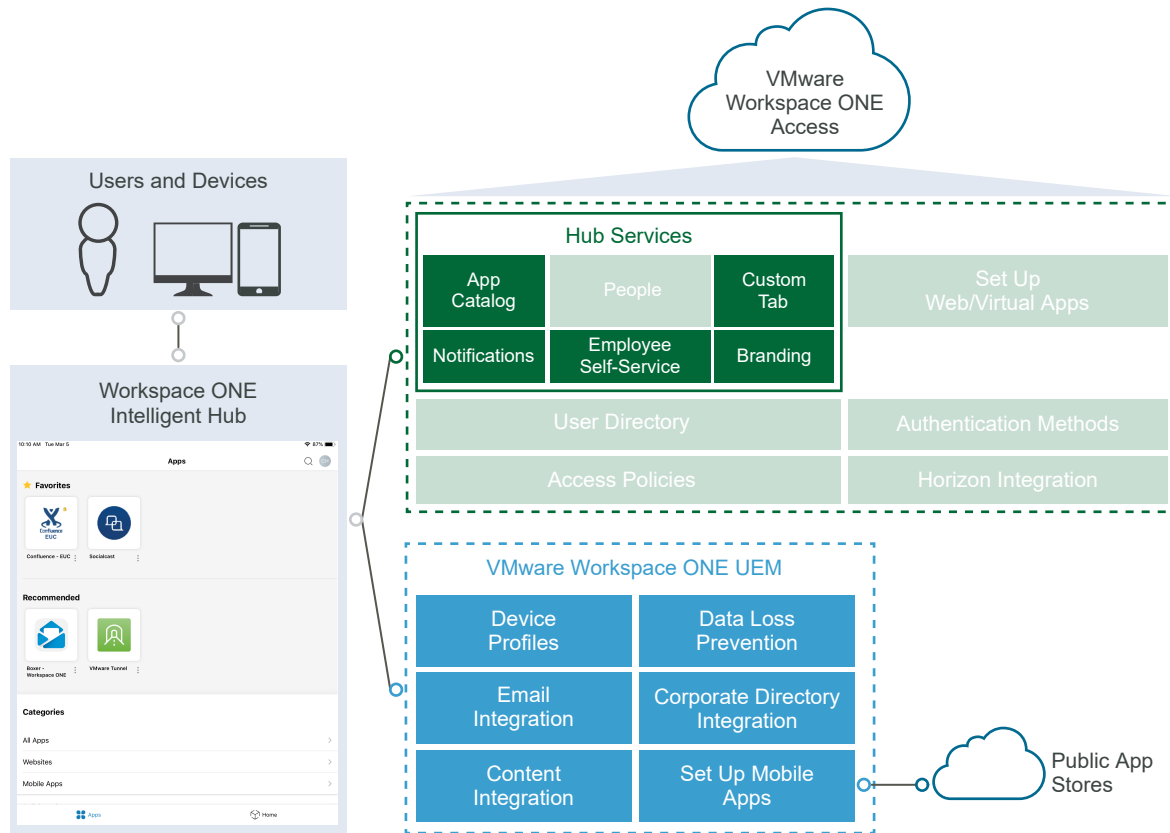
After you activate Hub Services for your cloud tenant, you can configure the Hub Services features that are supported with Workspace ONE UEM.

In Hub Services, you can customize the Hub Catalog layout, add a custom tab that displays with the catalog, and change the app branding to incorporate your company logo and colors.

The Workspace ONE UEM services provide device enrollment, application distribution, and mobile apps available from a public app store.

When the authentication mode is set to UEM, you can create notifications in Hub Services without integrating with Workspace ONE Access to send to the Workspace ONE Intelligent Hub app on iOS and Android devices. The Notifications functionality is enabled by default. Users see the notification on their devices and can open the notification and take action directly on the notification page. See [Chapter 8 Using Hub Notifications Service in Workspace ONE Hub Services](#).

Figure 3-1. Workspace ONE UEM with Hub Services



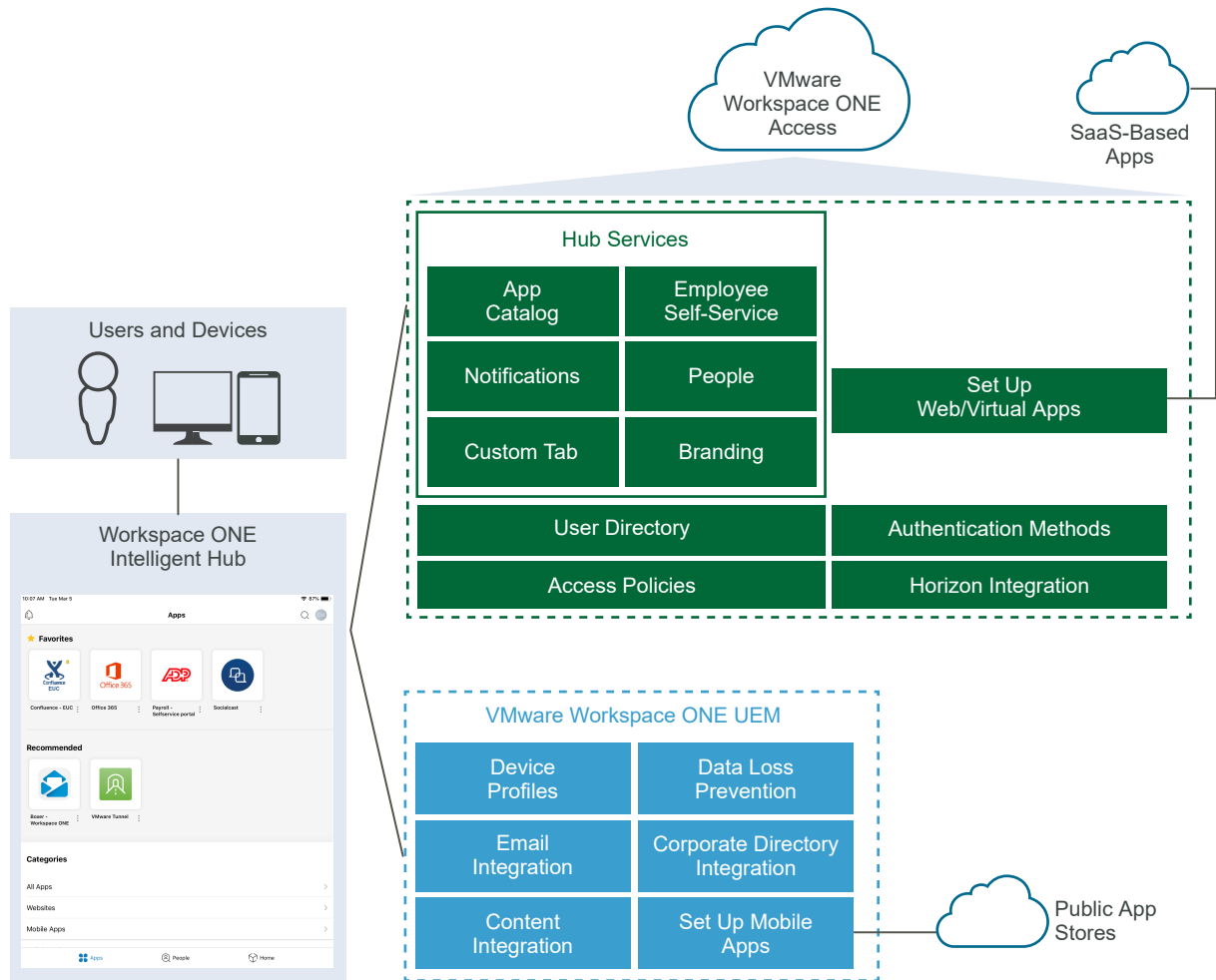
In the Workspace ONE UEM console, go to the **Groups & Settings > Configurations > Intelligent Hub** page to enable Hub Services. See [How to Activate Hub Services](#).

Using Hub Services When Workspace ONE Access Is Integrated

When Workspace ONE Access is integrated with Workspace ONE UEM, you can create a fully digital workspace experiences for users with additional Hub Services features including the People service and the Hub portal.

In addition, when Workspace ONE Access is integrated, the identity-related components are available, including authentication for users who use single sign-on to access their apps. You create a set of policies that relate to networking and authentication to control access to these apps.

Figure 3-2. Workspace ONE with Hub Services and Workspace ONE Access



Using Hub Services When Workspace ONE UEM and Workspace ONE Access Are Integrated

When Workspace ONE UEM and Workspace ONE Access are integrated, users from MDM-enrolled devices can sign in to the Workspace ONE Intelligent Hub app to access their resources securely without entering multiple passwords.

You install and configure the Workspace ONE Access connector component and integrate your company's Active Directory. In the Workspace ONE UEM console, you set the source of authentication for Hub to Workspace ONE Access.

When you integrate Workspace ONE Access, The Hub Services feature People can be configured. When the People functionality is enabled and configured in the Workspace ONE Access console, users can view organization charts and search for and contact colleagues directly from their device. The People functionality must be enabled and configured in the Workspace ONE Access console before you enable access to People in Hub Services. See [Set Up People Search in Workspace ONE Access](#).

In addition, the Hub Catalog can be expanded to include virtual apps such as VMware Horizon, VMware Horizon Cloud Services, and Citrix published apps, and other SaaS apps configured in the Hub catalog.

Note When you are integrated with Workspace ONE Access, to use the notifications builder wizard to create custom notifications for your organization, the role configured in the AirWatch API certificate that is used for authentication between Workspace UEM and Workspace ONE Access must be Console Administrator. You can verify the administrator role in the Workspace UEM console **Accounts > Administrators > List View** page.

Integrate Hub Services with Workspace ONE Intelligence to Share Hub Services Notification Analytics

Integrate your Workspace ONE Hub Services with VMware Workspace ONE[®] Intelligence[™] to enable the transfer of data between the two systems.

When you integrate with Workspace ONE Intelligence, you can view the analytics of end user's interactions with Workspace ONE Intelligent Hub notifications. Notification metrics includes create, sent, viewed, opened, dismissed and actioned on data. In Workspace ONE Intelligence, you can manage a custom dashboard to display analytics about your Hub Services notifications.

When you configure automation workflows in Workspace ONE Intelligence, you can leverage the Hub Services notification action to target and send Hub notifications to devices about apps, devices, remediation resources, and updates. The Hub notification appears in the For You tab in the Workspace ONE Intelligent Hub app or Hub portal.

See [VMware Workspace ONE Hub Services Integration](#) in the VMware Workspace ONE Intelligence Product guide about how to integrate Hub Services with Workspace ONE Intelligence.

Note Notification analytics are collected from Hub Web portal, Windows Hub, and macOS Hub.

Manage Admin Roles in Workspace ONE Hub Services

4

Hub Services uses role-based access control (RBAC) to manage administrator's access to the services in the Hub Service console.

Five predefined administrator roles can be assigned to Workspace ONE Access user groups in the Hub Services console Admin Roles page.

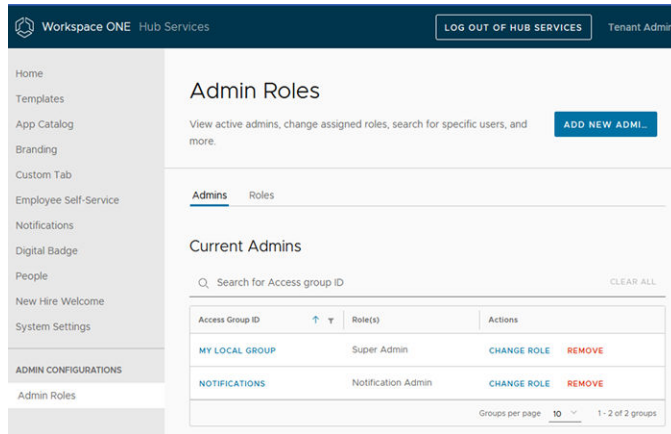
- **Super Admin.** The super admin role can access and manage all features and functions in the Hub Service console. Only super admins can assign and manage roles. The first super admin in Hub Services is the Workspace ONE Access super admin.
- **Auditor.** The auditor role has read-only permissions to view all pages in the Hub Service console.
- **Notification Admin.** The notification admin role can create and send notifications, manage the notification list on the Notifications List tab, and edit the Notifications Global Settings page.
- **Notification Creator.** The notification creator role can create and send notifications from the Notifications List tab. The notifications creator has read-only access to view the Global Settings page.
- **Notification Auditor.** The notification auditor role has read-only permissions to view the Notifications List tab and Notifications Global Settings page.

As a super admin, you can assign user groups which you created in the Workspace ONE Access console, to Hub Services admin roles. The members of the user group become administrators for that particular role. You can assign the same group to multiple roles, or assign different group to each role.

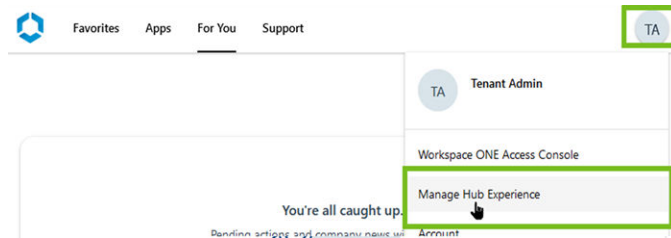
When a group is assigned to more than one role, the behavior of the roles applied is additive. For example, if the user group is assigned two roles, one is Auditor with read-only permission in the Hub Services console and the second role is Notification Admin, the group can view all the Hub Services console pages, and in the Notifications pages, can create, send, and manage notifications.

By default, admins that are granted the Notification Admin or Notification Creator role can manage and send notifications to any groups in your organization. When you add groups to a notification role, you can specify a specific target audience that the admins can send notifications to. When you select a specific target audience, you can ensure that admins are sending notifications to only that target audience. You can assign target groups from Organization groups, Smart groups, Workspace ONE Access User groups, and platforms.

You can see the list of the current admins groups and their roles, change a role, and remove roles from the Hub Services Admin Roles page.



Users that are assigned Hub Services admin roles access the Hub Services console directly from their Workspace ONE Intelligent Hub web portal. Users click on the user name in the Web portal and select the **Manage Hub Experience** link.



Hub Services Super Admin Role

The first super admin in the Hub Services console is the Workspace ONE Access super administrator. To add other super admin users, the Workspace ONE Access super admin assigns a Workspace ONE Access user group to the Hub Services super admin role. Members of the group can access and manage all features and functions in the Hub Services console, including adding groups to the other Hub Services roles. Members of the Hub Services super admin group do not have permissions to access the Workspace ONE Access console.

Workspace ONE Access admin users who are not super admins in Workspace ONE Access are designated as Auditor admins in the Hub Service console. In this role, they are granted read-only access to tabs, the notification list, and all notifications sent to any target audience.

Read the following topics next:

- [Add Workspace ONE Access User Groups to Admin Roles in Hub Services](#)
- [Adding Admin Groups and Assigning Customized Target Audience Permissions](#)

Add Workspace ONE Access User Groups to Admin Roles in Hub Services

As a super admin, you can add Workspace ONE Access user groups as admins in the Hub Services console and assign a RBAC access role. You can assign more than one role to a user group.

Prerequisites

Identify the user groups in the Workspace ONE Access services to assign to the admin roles.

Procedure

- 1 Navigate to the Hub Services console **Home** page.
- 2 Click **Admin Roles**.
- 3 In the **Admin Roles** page, click **ADD NEW ADMIN**.

The screenshot displays the Workspace ONE Hub Services interface. The top navigation bar includes the Workspace ONE logo, 'Hub Services', a 'LOG OUT OF HUB SERVICES' button, and the user role 'Tenant Admin'. The left sidebar contains various navigation options, with 'Admin Roles' under 'ADMIN CONFIGURATIONS' highlighted by a green circle with the number 1. The main content area is titled 'Admin Roles' and includes a sub-header 'View active admins, change assigned roles, search for specific users, and more.' A blue 'ADD NEW ADMIN' button is highlighted with a green circle and the number 2. Below this, there are tabs for 'Admins' (selected) and 'Roles'. The 'Current Admins' section features a search bar for 'Access group ID' and a 'CLEAR ALL' link. A table lists the current admins with columns for 'Access Group ID', 'Role(s)', 'Target Audience Permissions', and 'Actions'.

Access Group ID	Role(s)	Target Audience Permissions	Actions
NTF_GROUP	Auditor	CUSTOM ACCESS	EDIT REMOVE
NTF_TEST_GROUP	Notification Creator	CUSTOM ACCESS	EDIT REMOVE
PEN-TESTING-USER-GROUP	Notification Admin	Full Access	EDIT REMOVE

At the bottom of the table, there is a pagination control showing 'Groups per page 10' and '1 - 3 of 3 groups'.

- 4 Enter the Workspace ONE Access group name in the Step 1 search box and select the user group.

Add a new Admin

View active admins, change assigned roles, search for specific users, and more.

Step 1: Enter an Access group ID

Start typing an Access group ID

Step 2: Assign a role. You can select Super Admin, or you can select one or more Sub Admin roles.

Super Admin
 Full access to services, templates, Hub Services admin console.
[VIEW PERMISSION](#)

or

Auditor
 Read access to all services and templates.
[VIEW PERMISSION](#)

Notification Auditor
 Read access for Notifications
[VIEW PERMISSION](#)

Notification Creator
 Read access for Global Settings, create and send notifications.
[VIEW PERMISSION](#)

Notification Admin
 Read and write access to all Notification features.
[VIEW PERMISSION](#)

Change Target Audience

This admin group can send notifications to all audience groups.

[EDIT](#)

Target Audience Type	Access Permissions
Workspace ONE Access user group	Full Access
Organization Group	Full Access
Smart Group	Full Access
Platform	Full Access

- 5 In step 2, select the role to assign.

By default, when creating a notification, admins can select to send a notification to any of the audience types listed in the Notification Builder, including all devices, all employees, organization groups, smart groups, and user groups. If this admin group can send notifications to all target audiences, do not edit the Custom Target Audience Section. To set a custom target audience, see [Adding Admin Groups and Assigning Customized Target Audience Permissions](#).

- 6 Click **ADD**.

The group is added to the Current Admins list and members of the group can log in to the Hub Services console from their Workspace ONE Intelligent Hub web portal.

What to do next

Notify the members in the group about their granted permissions and how to log in to the Hub Services console from the Manage Hub Experience link on the Hub portal browser.

Adding Admin Groups and Assigning Customized Target Audience Permissions

Roles-based access control lets you restrict the target audience that is managed in admin roles in Hub Services. When you restrict the target audiences to a specific type of audience, admins are granted permission to send notification only to that target audience.

When an admin creates a notification in the Notification Builder, the Notification Builder only shows the target audience types and groups that are granted to this admin group. They can also view and take actions on notification sent to the custom target audience types.

When adding an admin group to a notifications role, you can select Organization groups, Workspace ONE Access User groups, Smart groups, and platform as target audience types. For each audience type, you can either grant admins full access to all members of that audience, or you can configure a custom access and select specific groups in the target audience that can receive notifications. For example, you can grant the global communications team Full Access to send notifications to all organization groups in your company and grant the United States communications team Custom Access to sending notification only to organization groups in the United States.

Change Target Audience

This admin group can send notifications to all audience groups.

[EDIT](#)

Target Audience Type	Access Permissions
Workspace ONE Access user group	Full Access
Organization Group	Full Access
Smart Group	Full Access
Platform	Full Access

Prerequisites

Identify the user groups in the Workspace ONE Access services to assign to the admin roles.

Procedure

- 1 Navigate to the Hub Services console **Home** page.
- 2 Click **Admin Roles**.
- 3 In the **Admin Roles** page, click **ADD NEW ADMIN**.

The screenshot shows the Workspace ONE Hub Services console. The top navigation bar includes the logo, 'Workspace ONE Hub Services', a 'LOG OUT OF HUB SERVICES' button, and the user role 'Tenant Admin'. The left sidebar contains various navigation options, with 'Admin Roles' under 'ADMIN CONFIGURATIONS' highlighted with a green circle and the number 1. The main content area is titled 'Admin Roles' and includes a description: 'View active admins, change assigned roles, search for specific users, and more.' A blue 'ADD NEW ADMIN' button is highlighted with a green circle and the number 2. Below the title, there are tabs for 'Admins' (selected) and 'Roles'. A search bar is present with the placeholder text 'Search for Access group ID' and a 'CLEAR ALL' link. The main content is a table with the following data:

Access Group ID	Role(s)	Target Audience Permissions	Actions
NTF_GROUP	Auditor	CUSTOM ACCESS	EDIT REMOVE
NTF_TEST_GROUP	Notification Creator	CUSTOM ACCESS	EDIT REMOVE
PEN-TESTING-USER-GROUP	Notification Admin	Full Access	EDIT REMOVE

At the bottom of the table, there is a pagination control showing 'Groups per page 10' and '1 - 3 of 3 groups'.

- 4 Enter the Workspace ONE Access group name in the search box to select the user group and select the Notification role to assign.

1 Start typing an Access group ID

Step 2: Assign a role. You can select Super Admin, or you can select one or more Sub Admin roles.

Super Admin
Full access to services, templates, Hub Services admi...
[VIEW PERMISSION](#)

or

2

Auditor
Read access to all services and templates.
[VIEW PERMISSION](#)

Notification Auditor
Read access for Notifications
[VIEW PERMISSION](#)

Notification Creator
Read access for Global Settings, create and send...
[VIEW PERMISSION](#)

Notification Admin
Read and write access to all Notification features.
[VIEW PERMISSION](#)

- 5 In the **Change Target Audience** section, click **Edit**.

By default, all target audiences are enabled with full access. You can deactivate any of the target audience types. You can change Full Access to Custom Access and enter the specific target audience name for custom access.

- **Full Access** grants admins full permissions to all groups or platforms in the target audience type. For Workspace ONE Access user groups, this included **All Employees** as a group and for Smart Groups, this includes **All Devices** as a group.
- **Custom Access** gives super admins the ability to select one or more groups or platforms to assign. The super admin can select **All Employees** or **All Devices** as an audience type option when they enable **Custom Access**.

To customize the target audience settings, deactivate the Access toggle for audiences you do not want in this role. To set up the notification role for a specific audience type, select **Custom Access** and enter the group name or platform.

Change Target Audience ✕

Select access level and corresponding group(s) below.

Target Audience Type	Access Level	Access On/Off
Workspace ONE Access user group	<input type="radio"/> Full Access <input checked="" type="radio"/> Custom Access <input type="text" value=""/> <small>Start typing the Workspace ONE Access user group name</small>	<input checked="" type="checkbox"/>
Organization Group	<input type="radio"/> Full Access <input checked="" type="radio"/> Custom Access <input type="text" value=""/> <small>Start typing the Organization Group name</small>	<input checked="" type="checkbox"/>
Smart Group	<input type="radio"/> Full Access <input checked="" type="radio"/> Custom Access <input type="text" value=""/> <small>Start typing the Smart Group name</small>	<input checked="" type="checkbox"/>
Platform	<input type="radio"/> Full Access <input checked="" type="radio"/> Custom Access <input type="checkbox"/> iOS <input type="checkbox"/> Android <input type="checkbox"/> Mac <input type="checkbox"/> Windows	<input checked="" type="checkbox"/>

6 Click **DONE**.

7 Click **Add**.

Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users

5

The initial configuration of the Hub Services feature settings for the Workspace ONE Intelligent Hub experience are the global settings that you configured to meet most of your users' needs. You create Hub templates with different Hub features and settings to provide a curated experience in Workspace ONE Intelligent Hub for different groups in your organization.

When you create a template, the template is initially configured with the global settings to simplify setting up the template. If the global settings for a feature do not meet all your needs, you can create versions of App Catalog, Branding, Custom Tab, and Employee Self-Service settings with different configurations. When you add the feature to the template, you replace the global settings with a version you created.

Feature	Versionable	Description
App Catalog	Yes	Create versions of the Hub catalog that are configured with different sets of apps and sections to promote.
Branding	Yes	Create different versions of branding for Workspace ONE Intelligent Hub to customize the logo and branding for different sets of users.
Custom Tab	Yes	Create versions of the custom tab, each with a different label, URL, and position on the navigation bar.
Employee Self-Service	Yes	<p>Create versions of the Employee Self-Service page to customize the type of self-service support available to different groups of users. Each version of the Employee Self-Service settings can be configured with a different tab label, different helpful links, and the option to manage devices from Workspace ONE Intelligent Hub.</p> <p>If you do not require a global setting for employee self-service, you can deactivate the global setting.</p> <p>Note that when you deactivate the global setting and you do not create a version of the setting, the feature is not available to be added to the template.</p>

Feature	Versionable	Description
Notifications	No	You cannot create versions of Notifications. The Notifications functionality is enabled as a global setting. If you do not want to use Notifications to contact all users in your organization, you can deactivate Notifications as a global setting. You then add the Notifications feature to individual templates. All notification settings are configured as global settings and are inherited by the templates. You cannot change these settings for individual templates. You can manage the New App Notifications settings in templates.
People	No	You do not create versions of the People setting. To manage which groups can access the People feature, you deactivate People as a global setting and enable the People setting in templates that can use the feature.

When users require Workspace ONE Intelligent Hub features that are different from the global configuration, you create templates. You can assign Workspace ONE UEM smart groups and Workspace ONE Access user groups in a template to group users based on their role, location, or other criteria.

Templates are organized in the Hub console Template page in priority order. This priority determines which template is applied when users or devices are assigned to multiple templates.

Examples of when to use templates.

- Test your Intelligent Hub configuration with a small group of users before you roll it out to the company. Assign the template to a small group of users and expand the roll-out over time to give you an opportunity to receive user feedback and to control the communication.
- Brand each of your subsidiary companies with different logos and colors.
- Create custom tabs for different departments in your organization.
- Enable Notifications only in specific locations.

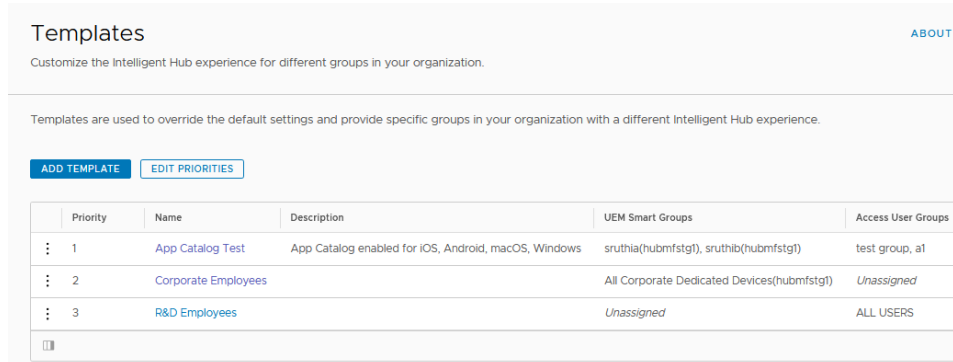
When you make a change to template settings, such as change the priority or reassign a template, users see the changed settings in Workspace ONE Intelligent Hub either when they restart the Workspace ONE Intelligent Hub app or when the Hub portal in the browser is refreshed.

Read the following topics next:

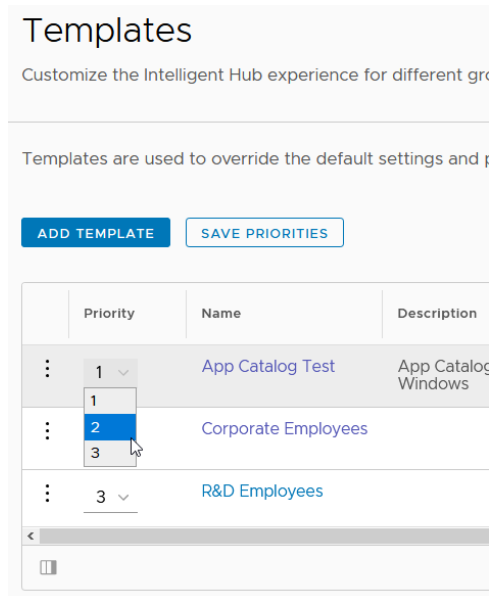
- [Managing Templates in Workspace ONE Hub Services](#)
- [How to Add a Template in Workspace ONE Hub Services and Assign It to Groups](#)
- [Configuring Templates to Restrict Access to Workspace ONE Intelligent Hub Features when Workers are Off Shift](#)
- [Adding an Onboarding Template and Preparing the Welcome Page for Pre-Hires in Hub Services \(Cloud Only\)](#)

Managing Templates in Workspace ONE Hub Services

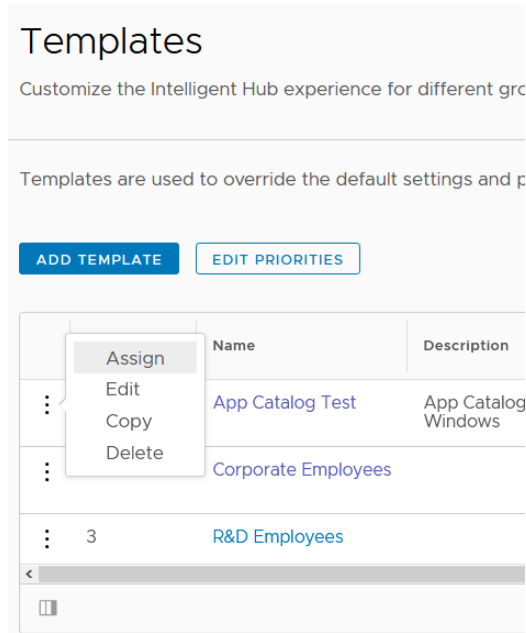
Templates that you create in the Hub Services Console are listed on the Templates page in a prioritized order with the highest priority listed first. This priority determines which template is applied when users or devices are assigned to multiple templates.



On the Templates page, you can add templates and change the priority.



You can assign groups to the template. You can edit, copy, and delete templates. When you copy a template, the assigned groups are not copied to the new template.



How to Add a Template in Workspace ONE Hub Services and Assign It to Groups

In the Hub Services console, you can set up one or more templates with specific Hub Services capabilities. You assign templates to different groups in your organization to define and control the Workspace ONE Intelligent Hub experience by group.

Which groups you can select to assign to a template depends on your Workspace ONE configuration.

- When the authentication mode is set to Workspace ONE UEM and Workspace ONE Access are not integrated, you can assign UEM smart groups. The Intelligent Hub experience on web browsers is not available.
- When the authentication mode is set to Workspace ONE Access and Workspace ONE UEM are integrated, you can assign UEM smart groups and Workspace ONE Access user groups. If you assign smart groups to a template, the template definition is available in the Workspace ONE Intelligent Hub app for iOS, Android, Mac, and Windows devices. Assign Workspace ONE Access user groups to the template to provide the same experience on web browsers. Assigning user groups with smart groups to a template provides a consistent experience for users across iOS, Android, Mac, and Windows devices and on a web browser.
- When Workspace ONE Access is not integrated with Workspace ONE UEM, you can assign user groups. In this case, the Workspace ONE Intelligent Hub experience on iOS, Android, Mac, and Windows is not available. Only the Hub web browser experience is available.

You can copy a template, change the name of the template, and change features sets. Copying a template simplifies the process to create a new template. When you copy a template, the assigned groups are not copied to the new template.

Prerequisites

- If Workspace ONE UEM is configured, Workspace ONE UEM must be version 20.08 or later to configure Templates in Hub Services.
- Workspace ONE Access on premise version must be 21.08 or later to configure Templates for on premises deployments.
- Make sure that the global Hub Services features and system settings are correctly configured.
- If you are not going to use a global setting in a template, create versions of the feature before creating the template. You can make versions for app catalog, branding, employee self-service page, and custom tab.

Procedure

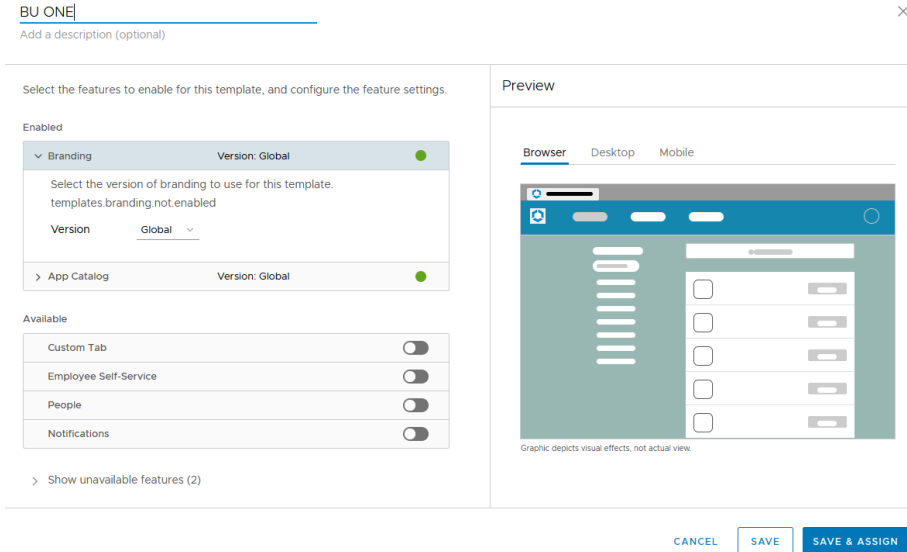
- 1 Navigate to the Hub Services console Home page and click **Templates**.
- 2 Click **ADD TEMPLATE**.

The New Template form displays. The new template is preconfigured with the global App Catalog and Branding settings.

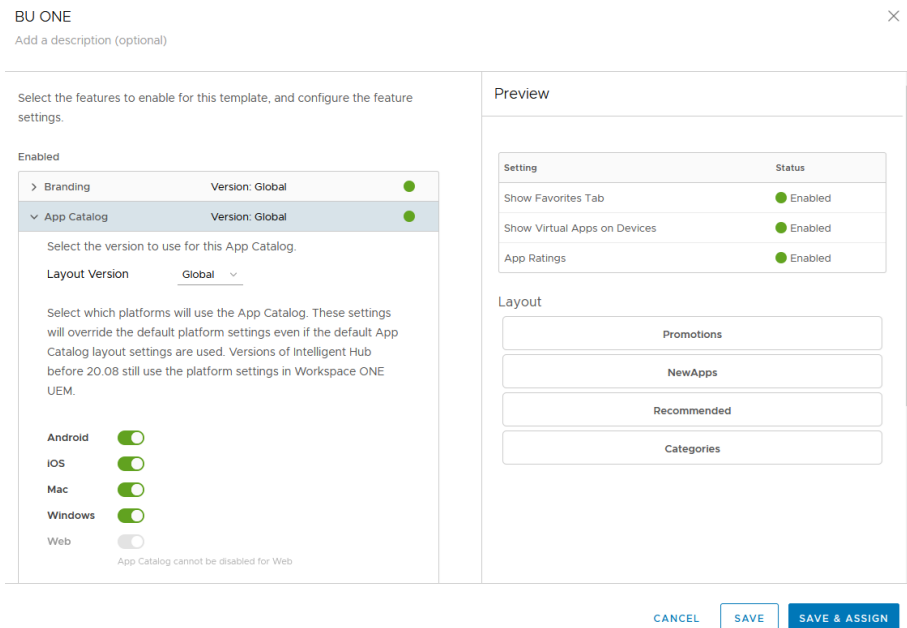
- 3 Click **New Template** and enter a name for the template.
Add a description of the template.

4 Review the **Enabled** section. Each feature configuration page includes a Preview section that shows how the feature is set up.


- a Click > to select the version of **Branding** to use in this template. The Global level setting is the default. In the Preview section, you can view the branding design.



- b Click > to select the version of the **App Catalog** layout to use in the template.
- c For **App Catalog**, select which platforms can use this app catalog layout.



- d Review any other features that are in the enabled section and select the version to use.

5 Review the **Available** section. To add a feature to the template, click . The feature is moved to the Enabled section.

6 Review the features that you move to **Enabled**.

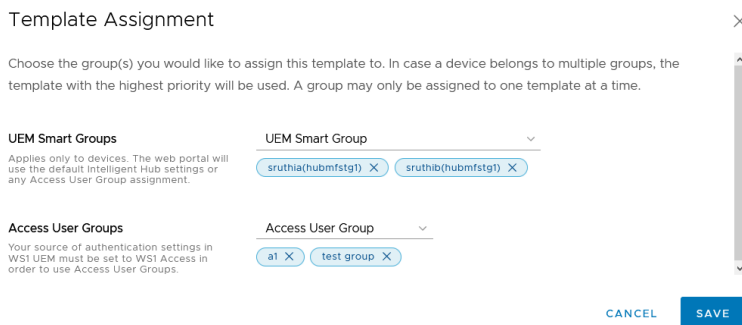
Features that are not set up in Hub Services global settings are not available to be used in the template and are listed in the **Show unavailable features** section.

7 If you are ready to save the template and assign it to a group, click **SAVE & ASSIGN**, otherwise click **Save**.

You can assign the template later from the Templates page.

8 Select the groups to assign to this template. Depending on your Workspace ONE deployment, you can select **UEM Smart Groups** and **Access User Groups**.

9 Click **Save**.



Template Assignment

Choose the group(s) you would like to assign this template to. In case a device belongs to multiple groups, the template with the highest priority will be used. A group may only be assigned to one template at a time.

UEM Smart Groups
Applies only to devices. The web portal will use the default Intelligent Hub settings or any Access User Group assignment.

UEM Smart Group

sruthia(hubmfstgt) X sruthib(hubmfstgt) X

Access User Groups
Your source of authentication settings in WS1 UEM must be set to WS1 Access in order to use Access User Groups.

Access User Group

a1 X test group X

CANCEL SAVE

The template is added to the bottom of the list on the Templates page.

When you make a change to template settings, such as change the priority or reassign a template, users see the changed settings in Workspace ONE Intelligent Hub either when they restart the Workspace ONE Intelligent Hub app or when the Hub portal in the browser is refreshed.

If you change the group that is assigned to a template or if you change the template priority, the change can take up to 8 hours to take effect on a device because the app is refreshed when the session token expires.

What to do next

Organize the templates in the Template page to prioritize the order that templates are accessed. When you set up multiple templates, prioritize the templates from the most specific user template to the more general.

Configuring Templates to Restrict Access to Workspace ONE Intelligent Hub Features when Workers are Off Shift

Shift-based access control with Workspace ONE enables your company to deliver a digital workspace that is shift aware. Shift-based access control restricts the use of different product apps and features when a worker is not clocked in for their shift. When Shift-based Access Control is configured, you can configure Hub Services templates to restrict access to some of the tabs in the Workspace ONE Intelligent Hub app or Hub portal when workers are not on shift, but let users continue to use other tabs.

You can enable **Restrict access during off-hours** in templates for the following tabs.

- Custom
- Employee Self-Service
- Notifications For You tab
- People

When you enable **Restrict access during off-hours**, the content in the tab is dimmed in the app or Hub portal view to show that it is not available.

Prerequisites

- Workspace ONE Access configured as the source of authentication.
- Shift-base Access Control configured in Hub Services

Procedure

- 1 Log into the Hub Services console and click **Templates**.
- 2 Click **ADD TEMPLATE**.
- 3 Name the template **Frontline Worker Access Control**.
- 4 To restrict access to Apps, Custom, Employee Self-Service, Notifications (For You), and People tabs in Workspace ONE Intelligent Hub app and Hub portal, expand each tab that you want to restrict and enable the toggle **Restrict access during off-hours**.

5 Click **Save and Assign**.

Add Template

Front-Line Worker Access Control [✎](#)

restricted access applied to notifications, Custom tab and people [✎](#)

Select the features to enable for this template, and configure the feature settings.

Enabled

> App Catalog	Version: Global	<input checked="" type="checkbox"/>
> Branding	Version: Global	<input checked="" type="checkbox"/>
> Custom Tab	Version: Global	<input checked="" type="checkbox"/>
> Employee Self-Service	Version: Global	<input checked="" type="checkbox"/>
∨ Notifications	All additional settings enabled	<input checked="" type="checkbox"/>
<p>Customize the settings for this template.</p> <p>New App Notifications <input checked="" type="checkbox"/> A weekly digest of new apps sent to employees. The first digest will be sent out one week after enabling.</p> <div style="border: 2px solid #00a651; padding: 5px;"> <p>Restrict access during off-hours <input checked="" type="checkbox"/> Notification alerts will be silenced during off-hours</p> </div>		
> People	Additional setting(s) enabled	<input checked="" type="checkbox"/>

- Start typing in either the **UEM Console smart group** or **Access user group** text box to assign the template to the group that is restricted access during off-hours.

Template Assignment ×

Choose the group(s) you would like to assign this template to. In case a device belongs to multiple groups, the template with the highest priority will be used. A group may only be assigned to one template at a time.

Workspace ONE UEM Console smart groups

Applies only to devices. The web portal will use the default Intelligent Hub settings or any Workspace ONE Access user group assignment.

Start typing the Workspace ONE UEM Console smart group name

Workspace ONE Access user groups

Your source of authentication settings in WS1 UEM must be set to WS1 Access in order to use Workspace ONE Access user groups.

Start typing the Workspace ONE Access user group name

CANCEL

SAVE

- Click **Save**.
- The template is added to the bottom of the list on the Templates page. Move the Frontline Worker Access Control template to first priority in the list.

Adding an Onboarding Template and Preparing the Welcome Page for Pre-Hires in Hub Services (Cloud Only)

You can customize the onboarding template in the Hub Services console to guide pre-hires to resources in Workspace ONE Intelligent Hub that can help them prepare to start working on day one. You set up the New Hire Welcome page to guide pre-hires through the steps to set up their account in your organization before their start date.

Note This feature is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

Workspace ONE Access with Hub Services provides a pre-hire onboarding experience through Workspace ONE Intelligent Hub on a web browser. Workspace ONE Access generates a one-time-use access token, called a magic link, that you send in an email to pre-hires. They click the link to access a Welcome page in the Workspace ONE Intelligent Hub portal.

You design and configure the New Hire Welcome page that pre-hires see when they click the magic link in the email they receive. The welcome page displays a pre-hire greeting and directions to set up their account and sign in to Workspace ONE Intelligent Hub portal in a web browser.

When you configure the onboarding template, the New Hire Welcome page, branding, and the Hub app catalog are enabled by default. If you created versions of branding and the Hub catalog specifically for pre-hire users, you edit the onboarding template to select the versions instead of using the global settings. You can enable Notifications if it is configured in Hub Services.

Note Employee Self-Service and People are not available for the onboarding template.

See [How to Prepare a Day Zero Onboarding Experience in Workspace ONE Intelligent Hub](#) for configuration details.

Customizing the Workspace ONE Intelligent Hub App Layout

6

You can modify the branding settings in Hub Services to add your company logo and change the colors that display in the Workspace ONE Intelligent Hub app or Hub portal in the browser. You can also add a custom tab to share company resources with users. The tab displays in the Workspace ONE Intelligent Hub app on Android and iOS devices or in the Hub portal.

Read the following topics next:

- [Adding a Custom Tab to Workspace ONE Intelligent Hub](#)
- [How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom Tab on the Web Portal](#)
- [Customize Branding for the Workspace ONE Intelligent Hub App and Hub Portal](#)
- [View Virtual Apps in Workspace ONE Intelligent Hub on Small Screens](#)
- [Manage Launch Screens that Display in Workspace ONE Intelligent Hub](#)

Adding a Custom Tab to Workspace ONE Intelligent Hub

You can configure a custom tab in the Hub Services console that can link to your company website or to another resource that you want to share with users. You can enable the custom tab to display in the Workspace ONE Intelligent Hub app on Android and iOS mobile devices and in the Hub web portal.

The custom tab feature is deactivated in the Hub Services global settings. You can enable this feature as a global setting and create different versions of the custom tab to use in templates. When you enable this feature, you can customize the label on the tab, add the URL of the destination, and select whether the custom tab displays in the first or last position in the app navigation bar.

When you enable the custom tab for the web, you select how the custom tab URL displays, either as a new tab on the navigation bar or in a Hub embedded iframe. When you select to use the Hub embedded iframe, the Hub Services console displays an iframe preview pane to use to verify that the URL loads correctly before you save the setting.

If the URL does not display correctly, you must change your web settings to give the web portal permission to embed your website in the iframe. see [How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom Tab on the Web Portal](#).

Add a Global Custom Tab

When you enable the custom tab, you select where the custom tab displays the tab displays on mobile devices and in the web portal.

- 1 Navigate to the Hub Services console Home page.
- 2 Click **Custom Tab**.
- 3 To set up a global custom tab that displays in the Intelligent Hub app, select **Enable Custom Tab**.
- 4 To display the custom tab in Workspace ONE Intelligent Hub app on mobile devices, enable **Android or iOS**.
- 5 To display the custom tab in the web portal, enable **Web** and select how the tab displays, as a **New Tab** or **Hub Embedded iFrame**.
- 6 Enter the name to display on the tab. The default label is **Home**.
Best practice is to create a label that is no more than six characters. Six characters or less display correctly on most types of devices.
- 7 Enter the URL address of the page that opens when users click this tab. Enter as **https://company.com**.
Users must be on a VPN to use the custom tab that is configured with an internal website like an intranet portal.
- 8 Select whether the custom tab is displayed first or last in the Intelligent Hub navigation bar.
- 9 If you selected Hub Embedded iFrame, check the preview pane to make sure that your URL displays correctly.
- 10 Click **Save**.

Create Versions of the Custom Tab

You can create versions of the custom tab. When you create templates, having different versions of the custom tab gives you the flexibility to customize the tab link based on the groups of users assigned the template.

- 1 Navigate to the Hub Services console Home page.
- 2 Click **Custom Tab**.
- 3 In the VERSION:GLOBAL menu, select **ADD VERSION**.
- 4 To display the custom tab in Workspace ONE Intelligent Hub app on mobile devices, enable **Android and iOS**.
- 5 To display the custom tab in the web portal, enable **Web** and select how the tab displays, as a **New Tab** or in a **Hub Embedded iFrame**.
- 6 Enter the name to display on the tab. The default label is **Home**.

Best practice is to create a label that is no more than six characters. Six characters or less display correctly on most types of devices.

- 7 Enter the URL address of the page that opens when users click this tab. Enter as **https://company.com**.

Users must be on a VPN service to use the custom tab with an internal website like an intranet portal.

- 8 Select whether the custom tab is displayed first or last in the Intelligent Hub navigation bar.
- 9 If you selected Hub Embedded iFrame, check the preview pane on the page to make sure that your URL displays correctly.
- 10 Click **Save**.

How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom Tab on the Web Portal

If you selected to use the Hub Embedded iFrame setting to display your custom tab URL and your website does not appear correctly in the Hub web portal, you can configure your web server to permit your website to appear correctly in the iframe.

How to Allow Your Website to Display in an iFrame in the Custom Tab on the Hub Web Portal

If your custom tab is not loading correctly in the iframe on the Hub portal, your website might be configured with the HTTP response headers X-Frame-Options or Content-Security-Policy to prevent your website from appearing in an iframe.

If the HTTP header **X-Frame Option** is configured for your website, to allow your website to display in an iframe, remove the X-Frame-Option header from your website configuration.

If the HTTP header, **Content-Security-Policy** is configured for your website, to allow your website to display in an iframe, add the `frame-src` option to the header to allow the web portal to embed your website in the iframe. Enter as

```
Content-Security-Policy: frame-src <https://YOUR-HUB-APP-URL>;
```

How to Configure Cross-Origin Resource Sharing (CORS) to Display Images Correctly in the Custom Tab on the Hub Web Portal

If images are not loading correctly in the iframe in the web portal, configure your website to allow the web portal to access images.

Images might not display because, for security, browsers restrict cross-origin HTTP requests initiated from scripts. This means that a web application using those APIs can only request resources from the same origin the application was loaded from. To allow images from other origins to display correctly, the response from the other origins must include the right CORS headers.

CORS is an http-header based mechanism that defines a way in which a browser and server can interact to determine whether it is safe to allow the cross-origin request. When performing certain types of cross-domain requests, browsers that support CORS initiate an extra "preflight" request to the server hosting the cross-origin resources to determine whether they have permission to perform the action. In preflight, the browser sends headers that indicate the HTTP method and headers that are used in the actual request.

In response, the server sends back an **Access-Control-Allow-Origin** header with `Access-Control-Allow-Origin: *`, which means that the resource can be accessed from any (*) origin. To retrieve the image resource, a **GET HTTP** request is used, and the server sends back an **Access-Control-Allow-Method** header with an **Access-Control-Allow-Method: GET**, which means that the resource can be accessed over a GET HTTP request.

To display images correctly in the web portal, you define the following CORS preflight request headers on your website.

```
Access-Control-Allow-Origin: <YOUR-HUB-APP-URL>
Access-Control-Allow-Method: GET
```

For more information about configuring CORS, see the [Cross-Origin Resource Sharing](#) website.

Customize Branding for the Workspace ONE Intelligent Hub App and Hub Portal

You can use your organization's logo in the Workspace ONE Intelligent Hub app and on the Hub portal pages instead of the default Workspace ONE logo. You can customize the product name that displays in the web browser tab, and change accent font and background colors.

You can also add logo and an accent color that displays correctly when users who use iOS and Android devices configure their screens for dark mode.

You can create a global brand setting and then create different versions of the brand design to add to Hub templates.

Create a Global Customize Branding Setting

- 1 Navigate to the Hub Services console Home page.
- 2 Click **Branding**.
- 3 Edit the settings in the Branding page.

Use the color picker to select the hexadecimal color code. Click and drag on the circle in the color area to select the shade of the color. Use the slider to select the hue.

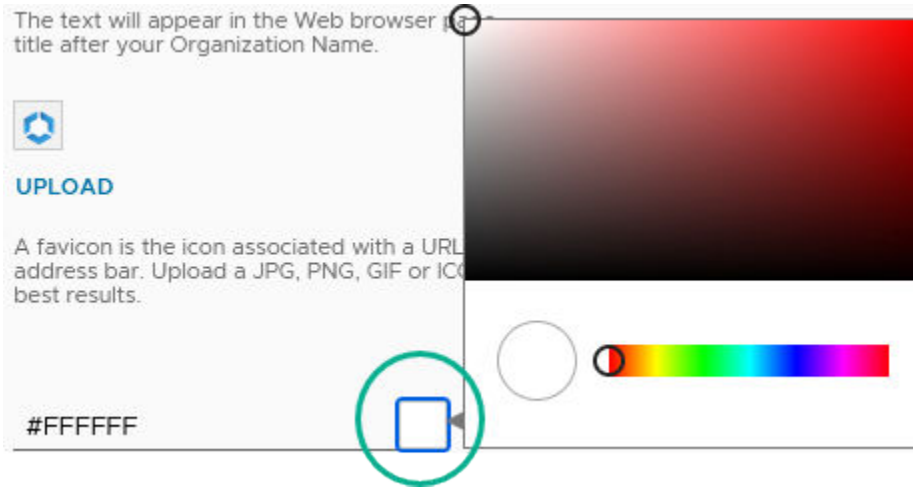


Table 6-1.

Option	Description
Logos	<p>Organization Logo. Click Upload to replace the current Workspace ONE Intelligent Hub logo that displays on the mobile, web browser, and desktop views. The format can be JPEG, PNG or GIF. For best display results, the maximum size of the image file is 10MB.</p> <p>Mobile App icon. You can change the color of the Workspace ONE Intelligent Hub app icon that displays on devices.</p>
Web Browser	<p>Organization Name. Enter the organization name to use as the title that displays in the browser tab. The default name is VMware.</p> <p>Product Name. Enter the text that displays after the organization name in the browser tab. The default name is Intelligent Hub.</p> <p>Favicon. A favicon is an icon associated with a URL that is displayed in the browser tab. The maximum size of a favicon image is 16 x 16 pixels. The format can be JPEG, PNG or GIF. Click Upload to upload a new image to replace the current favicon.</p>
Navigation Bar	<p>You can configure the appearance of the web browser navigation bar.</p> <p>Background Color. The default is white (#FFFFFF). Click the square next to the text box to use the color picker or enter a six-digit hexadecimal color code over the existing one to change the navigation bar background color.</p> <p>Font & Icon Color. Depending on your background color, select either Black or White for the text color.</p>

Table 6-1. (continued)

Option	Description
Tab Bar (Mobile)	Font & Icon Color <ul style="list-style-type: none"><li data-bbox="831 310 1374 401">■ Select Use Default branding to display the Intelligent Hub app text and icon colors that you configured for the Content.<li data-bbox="831 415 1398 470">■ Select Same as Navigation Bar to use the font and icon color configured for the Navigation Bar.

Table 6-1. (continued)

Option	Description
Content	<p>Accent Color. The accent color is the highlight color that is applied to links and active areas. For example, when a user selects a tab, the tab displays in the accent color. Click the square next to the text box to use the color picker or enter a six-digit hexadecimal color code over the existing one to change the color that displays around an app icon.</p> <p>Enable Advanced Content Branding Options for the following options.</p> <p>Background. You can select either Image or Color. If you select color, Background Color is displayed. The default is white (#FFFFFF). Click the square next to the text box to use the color picker or enter a six-digit hexadecimal color code over the existing one to change the background color in the body of the screen.</p> <hr/> <p>Note Do not select the same hex value for the accent color and background color. The app pages might not display correctly.</p> <hr/> <p>If you selected Background Image, upload the image to use as the background for the Hub portal page. The format can be JPEG, PNG or GIF. The image file size must be under 10MB.</p> <p>Font & Icon Color. Depending on your background, select either Black or White for the text color.</p>
Dark Mode	<p>Dark mode is a display setting on devices that displays a light color shade text against a dark or black screen. If users configure the dark mode setting on their iOS and Android devices, the Workspace ONE Intelligent Hub screens are displayed in dark mode. If users configure their computer settings to display screens in dark mode, the web browser displays the Workspace ONE Intelligent Hub screens in dark mode. Users can modify the appearance of their Hub web browser view from the Hub portal Account > Preferences page. The appearance set in the Hub portal Preferences page overrides the computer settings configured for light or dark mode.</p> <p>To provide end-users with the dark mode experience that aligns with your company's branding, configure your company dark mode logo and accent color.</p> <ul style="list-style-type: none"> ■ Dark Mode Organization Logo. Click Upload to replace the current dark mode Intelligent Hub logo with your logo. The format can be JPEG, PNG or GIF. ■ Dark Mode Background. You can select either Color Preset or Image. If you select Image, upload the background image. For best results, upload a JPEG, PNG, or GIF under 10 MB in size.

Table 6-1. (continued)

Option	Description
	<ul style="list-style-type: none"> ■ Navigation Bar Background Color. The default is black (#141414). Click the square next to the text box to use the color picker or enter a six-digit hexadecimal color code over the existing one to change the navigation bar background color. ■ Navigation Bar Font & Icon Color. The default font color is white (#FFFFFF). <hr/> <p>Note The Navigation Bar background color, font, and icon color settings are displayed in the Intelligent Hub web view.</p> <hr/> <ul style="list-style-type: none"> ■ Accent Color is the highlight color that is applied to links and active areas. Use lighter tones for better visibility on dark mode screens. <hr/> <p>Note If you do not configure a dark mode logo and accent color, the Workspace ONE Intelligent Hub app uses the default Intelligent Hub dark mode logo and accent color.</p>

You can see the changes that you make in the preview boxes on the right.

- 4 After you change the branding values, click **SAVE**.

If you want to return to the Workspace ONE Intelligent Hub default app settings, click **RESET**.

Create Versions of the Branding Setting for Templates

If the global branding design does not work for all your Intelligent Hub users, you can create versions of the branding design. Change the logo and colors to customize the look for different groups in your company.

- 1 Navigate to the Hub Services console **Home** page.
- 2 Click **Branding**.
- 3 Click the VERSION: GLOBAL down-arrow menu and select **ADD VERSION**.
- 4 Give this version a unique name and add an optional description.
- 5 Continue with Step 3 in the **Create a Global Customize Branding** section.

When templates are assigned to users, mobile device and macOS users see the new settings in the Workspace ONE Intelligent Hub app either when their session token expires and is refreshed or if they sign out of the Workspace ONE Intelligent Hub app and restart the app.

View Virtual Apps in Workspace ONE Intelligent Hub on Small Screens

Virtual apps such as Horizon and Citrix apps in the Workspace ONE Intelligent Hub app might not display correctly on small screen devices. To make sure that users have the best experience when they use virtual apps, you can deactivate the ability to view virtual apps on devices that have a screen smaller than 9 inches.

Procedure

- 1 Navigate to the Hub Services console **Home** page.
- 2 Click **App Catalog**.
- 3 Go to the end of the page and deselect **Show Virtual Apps on Devices**.
- 4 Click **Save**.

Manage Launch Screens that Display in Workspace ONE Intelligent Hub

When users enroll in to Workspace ONE Intelligent Hub, during the enrollment process, a series of screens are presented to show the high-level capabilities of Workspace ONE Intelligent Hub app features.

These introduction screens are enabled by default. You can deactivate this service from the Hub Services console > System Settings page.

Setting up the Workspace ONE Intelligent Hub App Catalog in Hub Services

7

The App Catalog in Hub Services lists the apps that you make available to your users in the Workspace ONE Intelligent Hub app or web portal. You can arrange the layout of the catalog page to make it easy to find apps from the Workspace ONE Intelligent Hub app and the Hub portal. You can add sections such as Categories or Favorites to organize apps, and you can enable App Rating to let users rate an app with a thumb up or down click.

The Apps tab displays the New Apps, Recommended, and Categories sections. You can customize the Apps tab view to add other sections.

Section	Description
New Apps	Apps that are added to the Hub Catalog display in the New Apps section for 30 days. New versions of an app are also displayed in the New Apps section.
Recommended	Preferred applications that you categorized as recommended in the catalog are displayed in the Recommended section.
Category List	The Categories section displays a list of the categories that you created. The categories display alphabetically by default. You can choose the order of these categories, moving the most important app categories to the top of the list.
Promotions	You can add a Promotions section to display apps that you want to promote to users. The Promotion section always displays at the top of the Apps pane.
Updates	You can add an Updates section to display a list of apps that have updates. Users can update the apps directly from the Updates section. Note The ability to display the Updates section is only available on iOS devices with Workspace ONE Intelligent Hub app version 21.06 and later.
Quick Actions	You can create a Quick Actions section and add on demand Workspace ONE UEM Freestyle Orchestrator workflows to this section. The Quick Actions section in the App catalog makes it easy for admins to place workflows that enable end users to configure their digital workspace quickly.
Custom	You can create custom category sections.

The Favorites tab is enabled as a separate tab that displays apps that users mark as a favorite. When the Favorites tab is enabled and Workspace ONE Access is the source of authentication for Workspace ONE Intelligent Hub, **Show Web Links** is also enabled to let users bookmark their favorite web links. Web links display in a separate section in the Favorites tab view. If you do

not want users to bookmark web links, you can deactivate the Show Web Link feature. If you deactivate the feature, the Web Links section does not display in favorites, but web links that users bookmarked are saved in Hub Services. If you re-enable Web Links, the saved web links reappear in the users Favorites view.

Read the following topics next:

- [Customize the Workspace ONE Intelligent Hub App Catalog in Hub Services](#)
- [Add a Promotions Section to the Catalog App View in Workspace ONE Intelligent Hub](#)
- [Add Featured Categories as Sections in the Catalog View](#)
- [Setting Up Quick Actions in App Catalog Tab \(Cloud only\)](#)
- [Managing Desktops and Apps That Display in the Workspace ONE Intelligent Hub App Catalog](#)
- [Create a Pre-Hire Version of the Hub Catalog for Workspace ONE Intelligent Hub](#)
- [Migrating Workspace ONE UEM App Catalog Settings to Hub Services](#)

Customize the Workspace ONE Intelligent Hub App Catalog in Hub Services

You can organize the Workspace ONE Intelligent Hub app catalog layout in the Hub Services console to promote apps, add different sections to display apps, and show the Favorites tab. You can also enable app ratings. The Hub Services out-of-the-box layout of the app catalog displays the New Apps section followed by the Recommended Apps section.

When you create the global Hub catalog settings, you select the platforms that can access the global catalog. The platforms options are Android, Apple iOS, macOS, and Windows Desktop. When Workspace ONE Access is integrated with Hub Services, the global catalog can be accessed from the Hub portal in a browser.

You can create versions of the catalog to target apps to different departments in your organization. For example, you can create a version of the app catalog for the HR group. For this app catalog, you promote apps that employees who work in HR use, and you add categories to the catalog that feature apps that are HR business-related apps. When you create a template for the HR group, you select the HR version of the catalog.

Create the Global App Catalog

Create the global app catalog so that the catalog is organized to apply to most group of users in your organization. When you create templates, you can assign the global app catalog to the template.

- 1 Navigate to the Hub Services console Home page.
- 2 Click **App Catalog**.
- 3 In the **Platforms** section, select which devices can be used to access the global Hub catalog.

- 4 Configure the **Catalog Layout** section.
 - a You can change the order that the New Apps and Recommended sections display in the Workspace ONE Intelligent Hub. Drag the six-dot icon to reorder the sections.
 - b To delete sections that you do not want to display, click **X**.
 - c If you want to promote a specific category, click **ADD SECTION** and select the category to display as a section in the Workspace ONE Intelligent Hub app.
- 5 **Show Favorites Tab** is enabled by default. If you do not want to include this tab in Workspace ONE Intelligent Hub, deactivate the setting. When the Favorites tab is deactivated, the Favorites tab and the Favorites section in the app catalog are not displayed.

When Workspace ONE Access as the source of authentication for Workspace ONE Intelligent Hub, the **Show Web Links** feature is also enabled. Users can bookmark web links that display in the Favorites tab. You can deactivate the Show Web Links feature.
- 6 (Optional) Enable **App Rating**, to allow users to rate the apps that they use.

When App Rating is enabled, thumb up and thumb down icons display in the User Rating section on the app details page.
- 7 Click **Save**.

Create Versions of App Catalog

Create versions of the app catalog to apply to a template when users have requirements that are different from the global catalog setup.

When you use templates to create versions of the app catalog, you do not select the platforms in the catalog settings. When you create the template, you enable the platforms that can use the version of the catalog.

- 1 Navigate to the Hub Services console Home page.
- 2 Click **App Catalog**.
- 3 In the VERSION:GLOBAL menu, select **ADD VERSION**.
- 4 Give this version a unique name and add a description.
- 5 Configure the **Catalog Layout** section.
 - a You can change the order that the New Apps and Recommended sections display in the Intelligent Hub. Drag the six-dot icon to reorder the sections.
 - b To delete sections that you do not want to display, click **X**.
 - c If you want to promote a specific category, click **ADD SECTION** and select the category to display as a section in the Workspace ONE Intelligent Hub app.
- 6 **Show Favorites Tab** is enabled by default. If you do not want to include this tab in Workspace ONE Intelligent Hub app, deactivate the setting. When the Favorites tab is deactivated, the Favorites tab and the Favorites section in the app catalog are not displayed.

When Show Favorites Tab is enabled, the **Show Web Links** feature is also enabled. Users can bookmark web links that display in the Favorites tab. You can deactivate the Show Web Links feature.

- 7 (Optional) Enable **App Rating**, to allow users to rate the apps that they use.
- 8 Click **Save**.

This version is added to the app catalog VERSION list.

Add a Promotions Section to the Catalog App View in Workspace ONE Intelligent Hub

You can add a Promotions section to the Hub Catalog to display featured apps at the top of the catalog view in the Workspace ONE Intelligent Hub app or the web portal.

Procedure

- 1 Navigate to the Hub Services console Home page.
- 2 Click the **App Catalog** page.
- 3 In the **Catalog Layout** section, click **New Section** to select **Promotions**.
The Promotions displays before Favorites in the App Catalog.
- 4 In the **Promotions** row, click > to expand the row.
 - a The default is to display Promotions in both the Workspace ONE Intelligent Hub app and the Hub web browser views. You can change the default.
 - b Select whether to promote apps or specific catalog categories.
 - c In the App/Category Name section, search for the names to promote.
Click **Add a row** to add additional names.
- 5 Click **Save**.

Add Featured Categories as Sections in the Catalog View

In the Hub Services console, you can create custom sections in the app catalog view based on categories you defined in Workspace ONE UEM or Workspace ONE Access. The custom category section displays the apps in the Intelligent Hub app catalog in the same way that New and Recommended sections are displayed.

Prerequisites

Make sure that you added the application categories in either the Workspace ONE UEM console or if integrated with Workspace ONE Access, the Workspace ONE Access console.

Procedure

- 1 Navigate to the Hub Services console Home page.

- 2 Click **App Catalog**, and select **ADD SECTION** .
- 3 Select **Custom** and in the **Search for a category** text box, select the category name that you want to feature.
- 4 To add another category select **ADD SECTION > Custom** again and select another category. Custom category sections display above the Categories section.
- 5 Click **Save**.

Results

If an application category that you feature is deleted from the Workspace ONE UEM or Workspace ONE Access consoles, the category is removed from the list in the console and in the users view of the app catalog.

Setting Up Quick Actions in App Catalog Tab (Cloud only)

You can create a Quick Actions section in the Workspace ONE Intelligent Hub Apps tab and add on demand Workspace ONE UEM Freestyle Orchestrator workflows to this section .

Note Quick Actions can be set up for Windows and MacOS devices only.

A Quick Actions section with the available quick actions is set up in the Apps page to make it easy for users to quickly find and execute workflows for problem-solving or configuring their digital workspace.

You use the Freestyle Orchestrator feature in the Workspace ONE UEM console to create customized workflows to automate endpoint configurations on Windows and MacOS devices. In Freestyle, you design a workflow, assign the workflow to the targeted platform, and select a smart group that can access the workflow. In the Workspace ONE UEM console, select **Show in Intelligent Hub** to deploy the workflow to the Hub catalog when the workflow is published.

You add Quick Actions as a section in the catalog App tab and select the workflows that are available as Quick Actions. When you make them available in the Quick Actions section, users can easily find, and access quick actions links for their Windows or MacOS device they are using.

Prerequisites

- Platform support for Windows 10 with Workspace ONE Intelligent Hub app 2404 or later
- Platform support for MacOS with Workspace ONE Intelligent Hub app 2404 or later

Overview of Using Freestyle Orchestrator to Create Workflows for Workspace ONE Intelligent Hub App Catalog

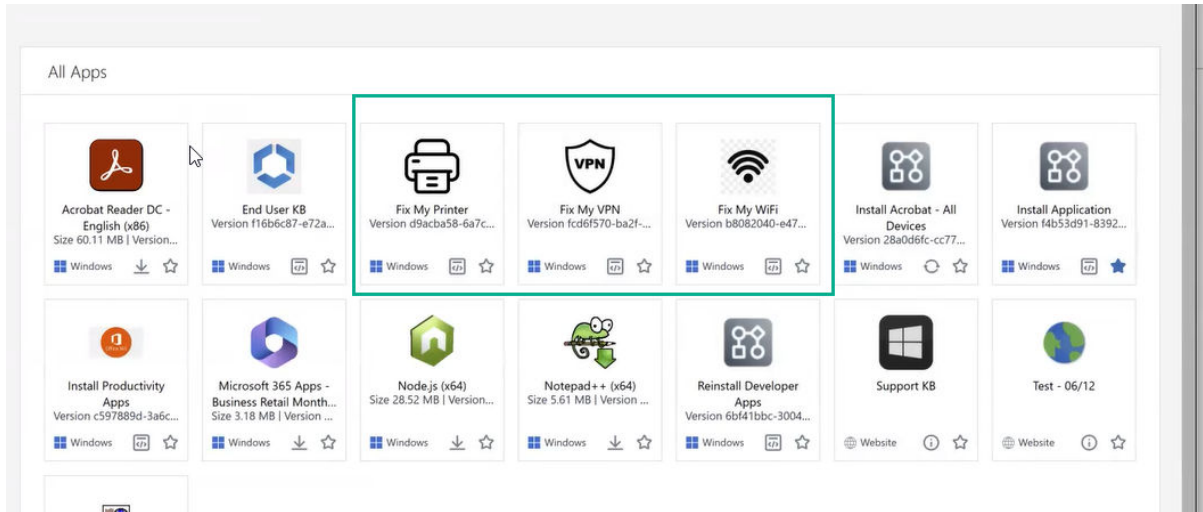
The following outlines the high-level steps in the Workspace ONE UEM console to create workflows that displays in the Hub App catalog. You can then select them to display in the Quick Action section in the App tab. See the [Freestyle Orchestrator guide](#) for detailed steps about creating and managing workflows.

- 1 In the Workspace ONE UEM console > Freestyle > Freestyle Orchestrator page, create a workflow.
- 2 In the **Admin Panel**, select the Windows platform and select the smart groups to which you want to assign the workflow.

The screenshot displays the 'ADMIN PANEL' for configuring a workflow. On the left, a workflow diagram shows two steps: '1 | Workflow Settings Windows' and '2 | Run Clear Google Chrome cache and...'. The right-hand panel contains the following configuration options:

- Workflow Settings**
 - Platform ***: Windows (Resources are filtered based on platform type.)
- Deployment Settings**
 - Select the Smart Groups that will be assigned to this workflow and how to deliver it.
 - Smart Groups ***: Add Smart Group (All Devices (uem-workflows-stg) X)
- Deployment ***
 - Auto Deploy
 - Show in Intelligent Hub
 - Auto Deploy and Show in Intelligent Hub
- Display Name ***: clear google cache v2
- Display Description (Optional)**: (Empty text box)
- Icon**: (Icon upload area with 'UPLOAD' button and file format restrictions: PNG, JPG or GIF, 1 MB maximum, 512 by 512 px recommended.)

- 3 In the **Admin Panel**, configure the Deployment setting **Show in Intelligent Hub**. When the workflows are published in the Workspace ONE UEM console, the workflows are displayed in the Workspace ONE Intelligent Hub Apps catalog. To make the quick action links easier to find, In the Hub Services console you can create a Quick Actions section to appear in the catalog Apps tab.



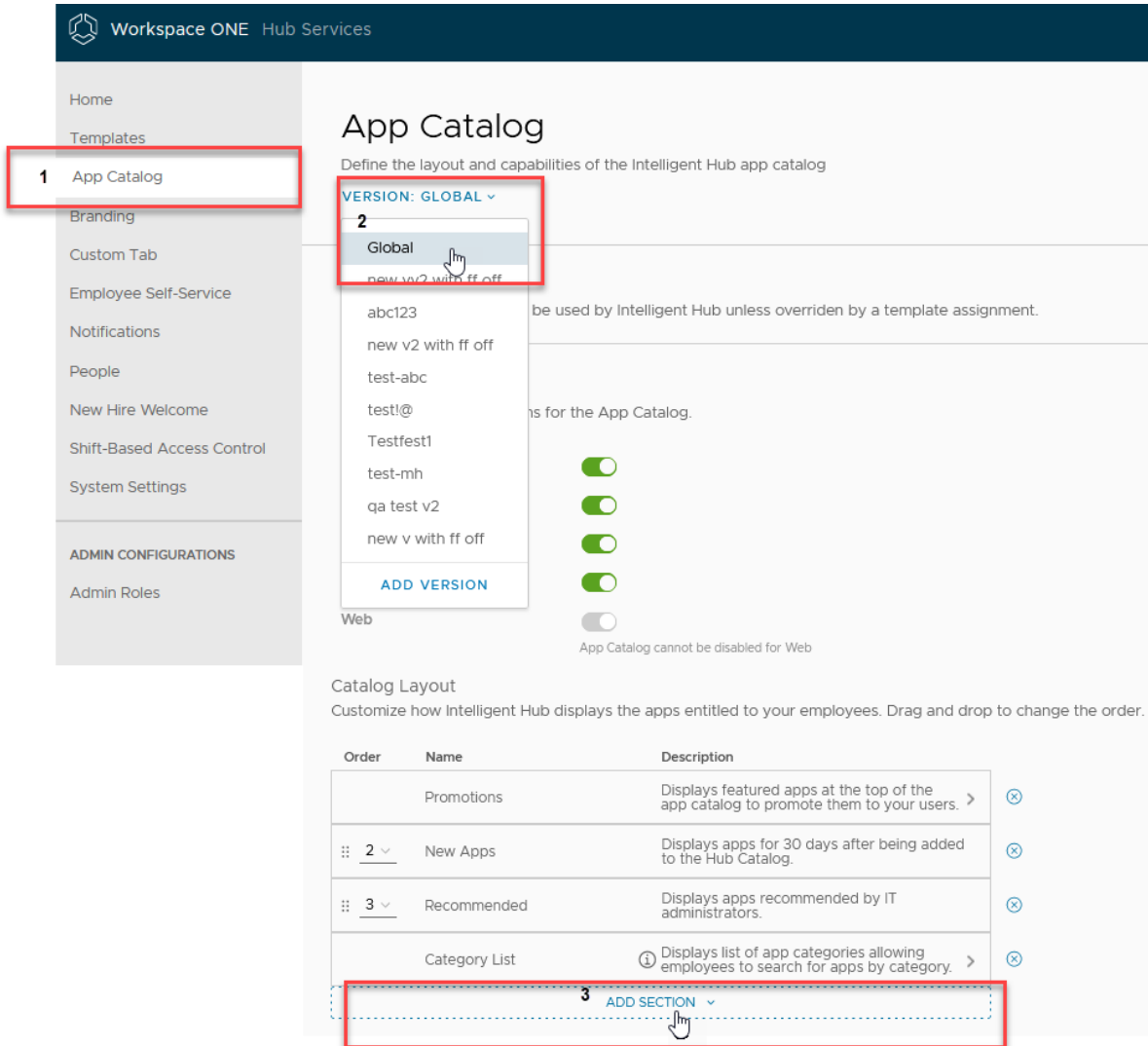
Configure Templates to Display Quick Actions Section in the Apps Catalog Tab

You can edit the Hub Services global and custom templates to add a quick actions section and add on-demand Workspace ONE UEM Freestyle Orchestrator workflows to this section. You can also create custom templates with quick actions in that are specific to the users in the smart groups that are assigned to that template.

For more information about how to set up templates in the Hub Services console, see [Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users](#).

Procedure

- 1 Navigate to the Hub Services console Home page and click **App Catalog**.
- 2 Select the version to edit, either GLOBAL to edit or create or edit a customized template.



- 3 In the App Catalog page, navigate to the **Catalog Layout** section and click **ADD SECTION**.
- 4 Select **Quick Actions**.
Quick Actions is added to the Catalog Layout table.
- 5 In the **Quick Action** row, click the arrow to open the search box.
- 6 Click **ADD A ROW** and click the down arrow in the **Search for quick action** search box to see a dropdown menu of the workflows. To search for a workflow, start typing in the search box. Select a workflow to add.
Click **ADD A ROW** to add additional workflows.

Catalog Layout
Customize how Intelligent Hub displays the apps entitled to your employees. Drag and drop to

Order	Name	Description
1	Quick Actions	Display the Quick Actions added
	Quick Actions	
	widnows-wf-4	
	shaftest - quickactions	
	macos-test-script	

ADD A ROW

Search for a quick action

- Clear Google Cache-1
- clear google cache v2
- Disk Clean up-1

7 (Optional) You can drag the six-dot icon to reorder where the Quick Actions section displays in the Apps tab.

8 Click **Save**.

Managing Desktops and Apps That Display in the Workspace ONE Intelligent Hub App Catalog

In the Workspace ONE Intelligent Hub app catalog, users can access applications and desktops that you manage from the Workspace ONE UEM console, the Workspace ONE Access console, the Horizon Console for the first generation of Horizon Cloud Services, and the Horizon Universal Console for the Horizon Cloud Service - next-gen.

Platform	Description
Workspace ONE UEM	<p>In the Workspace ONE UEM console, you configure, manage, and entitle to users cloud, mobile, and Windows apps that are publicly available from app stores and internal apps that are built in-house. See the Application Management Life-Cycle guide in the Workspace ONE UEM Documentation center.</p>
Workspace ONE Access	<p>In the Workspace ONE Access console, you configure, manage, and entitle uses to web apps and virtual apps. You can add some web applications to your catalog directly from the Workspace ONE Access catalog pages in the console. Other resource types require you to configure the resource outside the Workspace ONE Access console. See the Workspace ONE Access Resource Guide for information about setting up these resources in Workspace ONE Access.</p>
VMware Horizon Cloud Service – next-gen	<p>Prerequisite</p> <ul style="list-style-type: none"> ■ Workspace ONE Access is configured as the identity provider. ■ See the VMware Horizon Cloud Service – next-gen documentation for additional Horizon prerequisites. <p>(Cloud only) VMware Horizon Cloud Service – next-gen allows you to manage and monitor desktop and application deployments. When Workspace ONE Access is configured as the identity provider, you can enable Workspace ONE Intelligent Hub in the Horizon Universal Console Integrations > Workspace ONE Intelligent Hub page. Users can then access their Horizon desktops and applications in the App catalog pages from the Hub portal in a browser. When single sign-on is activated in the Horizon Cloud Service - next-gen, you can launch your desktop or app from the Hub portal without entering your credentials. See the VMware Horizon Cloud Service – next-gen documentation.</p> <p>Note Horizon desktops and apps assigned through the Horizon Cloud Service – next-gen cannot be accessed from the Workspace ONE Intelligent Hub app on iOS, Android, macOS, and Windows devices.</p>

Platform	Description
VMware Horizon Cloud Services - first-gen	When Workspace ONE Access is integrated with a Horizon Cloud tenant that has single-pod brokering enabled, you create one or more virtual apps collections in the Workspace ONE Access console. The virtual apps collections contain the configuration information for the Horizon Cloud tenants and sync settings. See Providing Access to VMware Horizon Cloud Services Desktops and Applications .
VMware Horizon Cloud tenant with Universal Broker enabled	(Cloud only) When Workspace ONE Access is integrated with a Horizon Cloud tenant that has Universal Broker enabled, the Hub Service syncs the Horizon Cloud entitlements directly from the Universal Broker service. See Horizon Cloud Environment with Universal Broker - Architecture of Integration with Workspace One Access and Intelligent Hub Services .
	Note Integration with Horizon Cloud Services on Microsoft Azure with Universal Broker is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the <i>Unsupported Workspace ONE Features</i> topic in the Configuring User Provisioning and Identity Federation with VMware Identity Services guide.

Create a Pre-Hire Version of the Hub Catalog for Workspace ONE Intelligent Hub

Create a version of the Hub catalog to be used in the pre-hire Workspace ONE Intelligent Hub onboarding experience. You apply this version in the onboarding template in the Hub console.

The pre-hire version of the catalog can be configured to display the selected apps that pre-hire users can access before their first day. The best practice is to simplify the navigation and features the pre-hire catalog as to not overwhelm the pre-hire experience in Workspace ONE Intelligent Hub.

Best practice design for the pre-hire catalog is to enable the Promotion banner to convey important apps that pre-hires can refer to and to give them access only to the apps that are relevant before day 0. To keep the catalog easy to navigate, deactivate features that can distract a pre-hire user, such as the category list, favorites tab and the ability to rate an app.

Procedure

- 1 Navigate to the Hub Services console Home page.
- 2 Click **App Catalog**.
- 3 In the **VERSION:GLOBAL** menu, select **ADD VERSION**.
- 4 Give this version a name, such as Pre-Hire General and add a description.

- 5 Configure the **Catalog Layout** section.
 - a Delete the **New Apps, Recommended,** and **Category List** sections.
 - b Deactivate the **Favorites** Tab.
 - c Leave **Show Virtual Apps on Devices** and **Enable App Ratings** deactivated.
- 6 In the **Promotions** row, click to expand the row.
 - a Leave the **Display the Promotions section** enabled.
 - b Select to promote **App** and then search for the apps to be promoted.
- 7 Click **Save**.

What to do next

Go to the Templates:Onboarding section and edit the template for the pre-hire Workspace ONE Intelligent Hub experience. Click App Catalog and select the Pre-hire version you created. See [Adding an Onboarding Template and Preparing the Welcome Page for Pre-Hires in Hub Services \(Cloud Only\)](#).

Migrating Workspace ONE UEM App Catalog Settings to Hub Services

Beginning with the Hub Services August 2020 Cloud and Workspace ONE UEM 2008 releases, management of the Workspace ONE UEM Hub catalog settings moves to the Hub Services console.

You can migrate your Workspace ONE UEM Hub catalog settings to the Hub catalog settings in the Hub Services console. Users' access to their Hub catalog through the Workspace ONE Intelligent Hub is uninterrupted.

During migration, your customer OG UEM app catalog settings are migrated to Hub Services and become the global level settings for the Hub app catalog. Hub templates are created for any child OGs with different settings from your customer OG settings. The Hub templates are assigned to UEM smart groups based on the user assignment in the OG.

If you do not want to migrate your Workspace ONE UEM Hub catalog settings, you can select to discard the migration option in the Hub Services console. If you select to discard the migration option, you cannot migrate your Workspace ONE UEM catalog. You can create Hub templates in the Hub services console, configure the Hub catalog settings, and assign Workspace ONE UEM smart groups to the templates.

Migration Process

When you migrate the Workspace ONE UEM Hub catalog settings to Hub Services, Hub templates are created based on your organization's deployment of the Hub catalog.

- The default global settings that are configured in Hub Services, including Branding, are applied to each template. If you do not want to use the global settings, you can customize the template.
- A Hub template is created during migration when child OGs is different from your customer OG. When the child OGs have the same configuration, but different users, only one template is created. For example, the customer OG hierarchy includes two child OGs, C1 and C2. C1 and C2 are configured with the same settings. The customer OG is configured with different settings. During the migration, Hub Services creates one template for C1 and C2 because they have the same configuration and assigns smart groups to the template .
- Smart groups are created based on the Workspace ONE UEM OG's assignment groups. The smart group settings mimic the OG settings.
- The platform settings that are enabled to access the Workspace ONE UEM Hub catalog are migrated to the Hub Services Hub catalog settings. You manage the platform settings for iOS, Android, Mac, or Windows in the template Hub catalog settings.
- Templates are prioritized in the Template list based on the OG hierarchy. The lower a child OG is in the OG hierarchy, the higher the associated template is listed in the Template list.

To learn more about Hub templates, see [Chapter 5 Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users](#) .

Migrate Hub Catalog to Hub Services

When Workspace ONE UEM is using Hub Services, you can migrate your app catalog settings to Hub Services.

Note If you select **Discard** in the Discard all App Catalog settings section on the Migration page in the Hub Services console, the Hub Template Migration Experience page is deleted, and you cannot migrate the Hub catalog settings from Workspace ONE UEM. You can manually set up Hub templates. See [How to Add a Template in Workspace ONE Hub Services and Assign It to Groups](#) .

- 1 To start the migration, log into the Hub Services console.
- 2 If your organization can migrate, you see the **Hub Template Migration Experience** screen.
- 3 In the Migrate all App Catalog settings section, click **MIGRATE**.
- 4 When the migration is complete, in the Next Steps section, click **FINISH**.

Go to the **Templates** page to see the prioritized list of templates that were created from the migration. You can re-prioritize templates, edit templates, assign different smart groups, and delete templates.

Your user access is uninterrupted. If you made changes to the branding or app catalog features in Hub Services, users see the changes when they sign in to Workspace ONE Intelligent Hub.

The catalog settings are removed from the Workspace ONE UEM console Groups & Settings > All Settings > Apps > Workspace ONE > AirWatch Catalog > General > Authentication tab or are displayed as read-only. The read-only settings in the Platform section that are listed on the page apply to older versions of Workspace ONE Intelligent Hub.

Using Hub Notifications Service in Workspace ONE Hub Services



The Hub Notifications service is a cloud-hosted service designed to generate and serve real-time notifications to your employees. In Hub Services, you can create custom informational and actionable notifications to send to selected groups in your organization.

You also have the out-of-box capability to send weekly new app notification to all employees, if you choose to turn it on.

Users do not need to be in the Workspace ONE Intelligent Hub app to receive notifications. They can respond directly on the notification that is being viewed. When users are logged in to Workspace ONE Intelligent Hub, they can view their notifications from the For You tab.

Source of Authentication Makes a Difference

When the source of authentication for Workspace ONE Intelligent Hub is set to Workspace ONE UEM, you do not need to configured Workspace ONE Access to create custom notifications.

- Users receive notification on their iOS, Android, macOS, and Windows devices.
- Users receive New App notifications for apps used on their devices.

When the source of authentication is set to Workspace ONE Access, you have additional notification features.

- Users receive notification cards on their iOS, Android, macOS, and Windows devices and in the Hub portal.
- Users receive New App notifications about web and virtual apps.

To see which service is the source for authentication in the Workspace ONE Intelligent Hub app, in the UEM console go to the Devices > Device Settings > Devices & Users > General > Enrollment > Authentication tab.

Note If you change the source of authentication from Workspace ONE UEM to Workspace ONE Access, notifications that were received from UEM are no longer available for viewing in the Workspace ONE Intelligent Hub app.

Read the following topics next:

- [Types of Notifications That Can Be Sent from Workspace ONE Hub Services](#)
- [Creating Custom Notifications in Workspace ONE Hub Services](#)

- [Action Methods That You Can Configure in the Workspace ONE Notifications API](#)
- [Archiving Notifications \(Cloud only\)](#)
- [Creating Notification Templates in Workspace ONE Hub Services](#)
- [Setting Up Push Notifications in Hub Services for Workspace ONE Access \(On Premises only\)](#)
- [Integrate Hub Services with Workspace ONE Intelligence to Provide Notification Analytics and Automation Workflows](#)

Types of Notifications That Can Be Sent from Workspace ONE Hub Services

You can create custom notifications from the Hub Services console Notifications page that display in the Workspace ONE Intelligent Hub app. In addition, you can create custom notifications with the Workspace ONE Notifications Service API.

Notifications	Description
New Apps Available Notification	<p>A New App notification to inform users about new apps that are granted to them is available with the Workspace ONE Intelligent Hub app.</p> <p>A new app notification message is automatically generated in Hub Services and sent weekly to employees. Users can select new apps and save them to their device from the notification message.</p> <p>If you do not want employees to receive the weekly notification, you can deactivate the New App Notifications setting in the Notifications Settings page.</p> <p>The new app notification message template cannot be modified.</p>
Custom Notification	<p>You can create custom notifications and set a notification priority in the Notification wizard in the Hub Services console or with the Notification APIs.</p> <p>When you use Notification wizard, two notification types are listed.</p> <ul style="list-style-type: none"> ■ Actionable. Actionable notifications require a user to take an action such as taking a mandatory training or approving an expense report. Select Actionable to send a notification that requires your users to respond in the notification. You can configure one to three actionable buttons when you create the custom notification. In the Additional Details section, you can add details about the notification. Additional details display in a label/ description format after the message. You can assign a due date that includes a day, time, and time zone by which the required action needs to be completed. The date displays on the notification card so users can see the when the action is required. ■ Informational. Informational notifications are notifications that do not require the reader to take action on the notification. New app notifications are displayed as informational notifications. <p>To use the Notification API to create custom notifications, go to the Workspace ONE Notification Service API page, https://code.vmware.com/apis/402#/Notifications. The Notifications Service reference guide is available from the Documentation tab on that page.</p> <p>When you create a notification, you can set the priority of the notification as either Standard, High-Priority, or Urgent.</p> <ul style="list-style-type: none"> ■ Standard. Notifications are sent as standard by default. When standard notifications are read or cleared from the screen, the notification count is reduced. ■ High- Priority. Notifications that are sent high-priority are displayed at the top of the For You notifications page within the Priority section. The notification count does not reduce until users mark the notification as read or act on the notification. ■ Urgent. Notifications that are sent as urgent are considered extremely important notifications that proactively alert users and require immediate attention or response. Users cannot proceed to another screen within the Intelligent Hub app until they take action on the notification. <p>You can target custom notifications to specific audiences, or you can send the notification to all employees in your organization. See Creating Custom Notifications in Workspace ONE Hub Services.</p>
Persistent Notifications	<p>Send persistent notifications when you want to alert users and you don't want them to dismiss the message. A persistent notification, also called a sticky notification, displays at the top of the For You page in the Workspace ONE Intelligent Hub app or Hub portal. Users cannot dismiss a persistent notifications, and it displays at the top of the For You page until the notification expires.</p> <p>If users receive more than one persistent notification, only the latest persistent notification is displayed. When that persistent notification expires, the next persistent notification that has not expired is displayed. After a persistent notification expires, it is moved to the History page.</p> <p>You create persistent notifications in the Notifications Service API. When you create the persistent notification in the API, you set the expiration date within the sticky object. See the Persistent Notification topic in the notification guide in the Workspace ONE Notifications Service API Documentation tab, and the hero card schema for more information.</p>

Creating Custom Notifications in Workspace ONE Hub Services

The notification builder in the Hub Services console guides you through the steps to create a notification, select the target audience, and create an actionable response. When you click **Create** in the wizard, the notification is sent to the target audience.

The type of notifications that can be sent are **Actionable** and **Informational**. See [Types of Notifications That Can Be Sent from Workspace ONE Hub Services](#).

You can also create and save commonly used notifications as notification templates. See [Creating Notification Templates in Workspace ONE Hub Services](#).

Who can send Notifications in Hub Services

Users who are delegated super admin permissions can send notifications to any audience.

In addition, super admins can assign user groups to predefined administrator roles to manage the Notifications services.

- **Notification Admin.** The notification admin role can create and send notifications, manage the notification list on the Notifications List tab, and edit the Notifications Global Settings page.
- **Notification Creator.** The notification creator role can create and send notifications from the Notifications List tab. The notifications creator has read-only access to view the Global Settings page.
- **Notification Auditor.** The notification auditor role has read-only permissions to view the Notifications List tab and Notifications Global Settings page.

When super admins assign user groups to a notification role, they can specify the exact target audience the admin can send notification to. When admins that are assigned a role with a custom target audience create notifications in the notification builder, the target audience field is pre-configured with the custom target audience name.

See [Chapter 4 Manage Admin Roles in Workspace ONE Hub Services](#).

Selecting the Target Audience

By default, notification admins can send notifications to the following target audience types in your organization.

Audience Types	Description
All Employees	Notifications can be sent to all employees listed as users in the Workspace ONE Access service.
All Devices	Notifications can be sent to all devices configured in your Workspace ONE UEM environment, regardless of organization groups.

Audience Types	Description
Organization Group	Organization groups (OG) in the Workspace ONE UEM console are created to group individual organizations in your corporate structure, geographical location, business unit, or department. You can select a specific organization group in Workspace ONE UEM in which to send the notification.
Smart Group	Smart groups are customizable groups within Workspace ONE UEM that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision. You can select a smart group in Workspace ONE UEM in which to send the notification.
Platform	You can select a specific platform type to send a notification. The platforms are iOS, Android, macOS, and Windows.
Users Group	Groups in the Workspace ONE Access service are imported from your Active Directory or are created as local groups in the Workspace ONE Access console. You can select a group in Workspace ONE Access in which to send a notification.

If your organization implements the pre-hire onboarding process, you might not want to send certain types of notifications to the pre-hire audience and groups. To exclude users in the pre-hire groups from receiving a notification, when you configure the target audience on the Definition page, select the **Exclude Pre-hires** check box.

Customized Target Audience Permissions

When the notification admin role specifies a specific target audience, an admin can have either Full Access to all users in the target audience or can have Custom Access and be given permissions to send notifications to selected group of users. The target audience types that can be select are shown in the following figure.

Target Audience Type	Access Permissions
Workspace ONE Access user group	Full Access
Organization Group	Full Access
Smart Group	Full Access
Platform	Full Access

- When an admin has Full Access permissions, they can send notifications to all groups or platforms in the target audience type. If Workspace ONE Access user group is selected as the target audience, full access includes **All Employees** as a group. If Smart Group is the target audience, full access includes **All Devices** as a group.
- When an admin has Custom Access permissions in a target audience, specific groups or platforms are assigned as the target audience type. **All Employees** or **All Devices** can be selected as a custom access option.

When an admin role includes custom target audiences, the notification builder shows only the target audience types and groups that the admin has permissions to access.

Actions That Can Be Added to Notification Messages

At the most, three actions can be presented on the notification card. When you create an action, a button appears with the text you configured. The ideal user experience is to have one or two actions. Any more than three can degrade the user experience as the buttons are in a horizontal line on the card, and the card can be too narrow to display the action buttons correctly.

Three action types can be selected.

- **Open In.** When you select the Open In action, you then enter the URL that opens when the button is clicked.
- **API.** When you select API, you then select the method to use to interact with the data being addressed in the notification.

API	Task Description
GET	Use GET to retrieve data from a specified resource. The data is not modified. Enter the URL of the resource that supplies the data.
POST	Use POST to send data to a specified URL to insert data in a resource. Enter the URL where the data is sent.
PUT	Use PUT to send data to a specified URL to update a resource. Use PUT when user can only send the data one time.

API	Task Description
PATCH	Use PATCH to allow users to modify their data on the resource.
DELETE	Use Delete to let the user delete data from the specified URL.

- **API with Parameters.** When you select API with Parameters, in addition to selecting the method and API endpoint, you can add specific parameters and a value for the parameters.

For more information about parameters, go to the [Workspace ONE Notification service API page](#). The Notifications Service reference guide is available from the Documentation tab.

Adding Attachments

You can add up to 10 attachments to notification that you create. The individual file size cannot exceed 5 MB.

Adding an Image, Video, and Links to Notifications

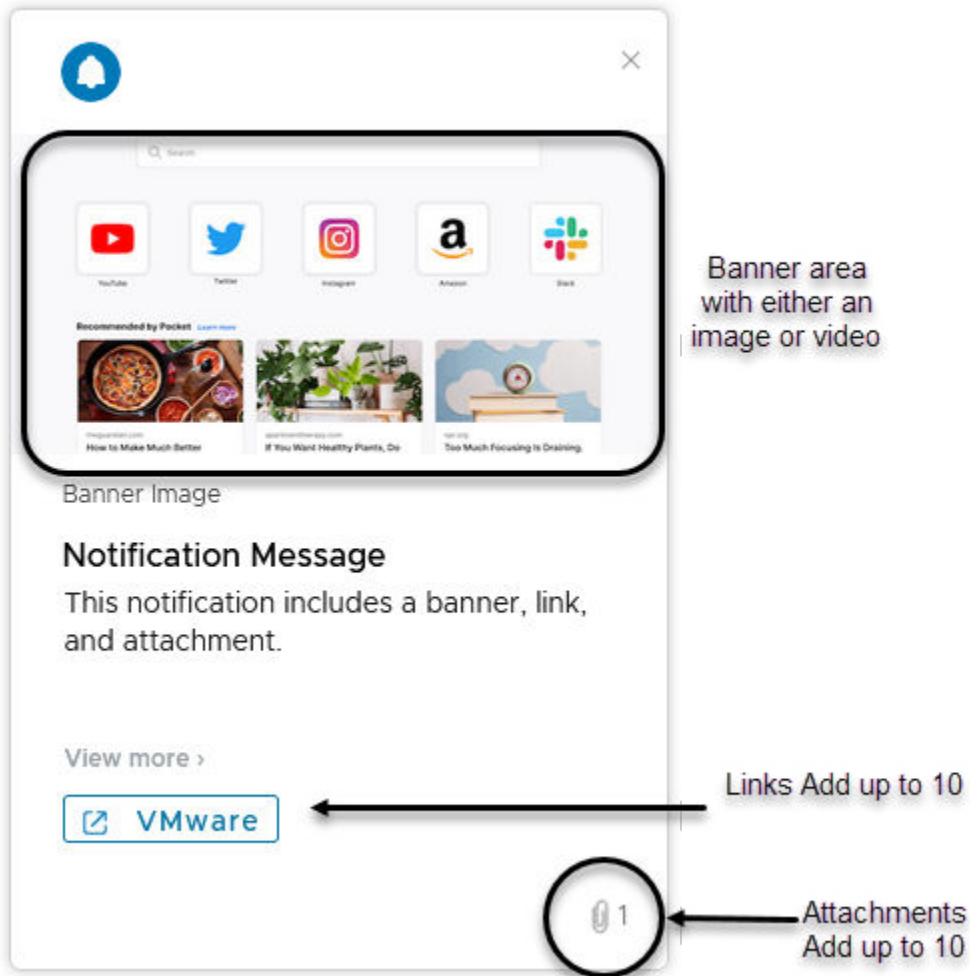
You can select to add an image or a video that displays as a banner in your notification and links that display in the **View more** section of the notification.

- To allow images and videos to display correctly in the notification banner, configure the web portal to permit cross-origin access to image or video files. You configure the following Cross-origin Resource Sharing (CORS) request headers on your website.

```
Access-Control-Allow-Origin: <YOUR-HUB-APP-URL>
Access-Control-Allow-Method: GET
```

- To display an image in the notification banner, enter the full URL address that includes HTTPS. Example of a full image URL address, `https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png`. The image must be either a JPG or PNG file and the aspect ratio of the image is 4:3.
- To display a video in the notification banner, enter the full URL address that includes HTTPS that is displayed in the embedded code as the `src` value. For example, `<source src="https://mozilla/media/videos/abcvideo.mp4">`.
- To add links to the notification, you add the link title that displays in the notification and then the complete link URL. You can add up to 10 links.

Figure 8-1. Notification Example with Banner, Links and Attachments



Notification Delivery Time

When you use the wizard to create a notification, when you click **Create**, the notification is created and sent.

The time it takes for the target audience to receive a notification depends on various factors. These factors include the Workspace UEM Mobile Device Management API response time and the total number of users and devices targeted for the notification. On an average, you can expect 10,000 recipients to receive the notification within 45 minutes.

Guidelines for Creating User-Friendly Notifications

Notifications cards include a header and message. The notification can also include buttons that make the message actionable. When you compose a message, consider the following good practices.

- Write short titles to catch the users' attention.

- Make the description message clear and concise.
- Use the **Additional Details** section to list details with a Label/Description that you would like to call out. Examples of types of additional details to add.
 - Author:Name
 - Phone number:XXX-XXX-XXXX,
 - Source:Technical Marketing
- No more than three actions can be presented on the notification card. One or two actions are the ideal user experience.
- When you create a label for your action button, keep it short to avoid truncation.
- If the user can repeat the action, enable the **Repeatable** radio button in the Content page. When the radio button is deactivated, users can perform the action once.
- The action buttons appear as either primary or secondary. The primary action button appears before a secondary action button.

In the default view of a notification message, a logo image appears in the left corner of the notification. You can change this image when you create a custom notification. You can upload an image or add a URL address to an image you want to appear on the card.

Change the Branding of Notifications Sent from Workspace ONE Hub Services

You can change the branding on notifications to add your company logo to the notifications you send through Hub Services.

You can configure your logo as the default image that displays in notifications instead of using the Intelligent Hub logo.

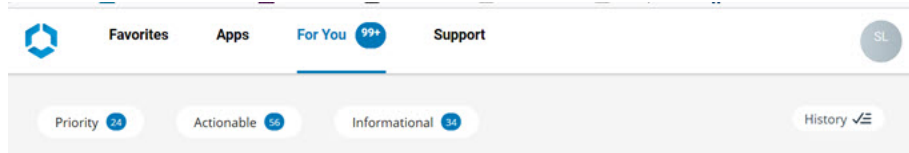
In the Hub Services console, go to the Notifications > Settings page to upload your image.

You can also add an image when you are composing custom notification content. The image you upload is used only for that message.

You can upload a JPG, PNG, GIF, or SVG file that is 40 px by 40 px. The image file cannot exceed 30 KB.

How Hub Services Notifications Display on User Devices

To make it easy for users to find messages on their devices, the messages are grouped on the **For You** page in the Workspace ONE Intelligent Hub according to the type of notification: Priority, Actionable, or Informational. If users do not have a notification from one of these types, that label is not displayed.



Urgent messages display outside of those groupings. Users cannot proceed to another screen until urgent notifications are acted on.

Users can see the number of notifications they have in the For You tab. This count represents the number of read or unread priority and actionable notifications, and the number of unread informational notifications. When Informational notifications are displayed in a page view, they are considered read without any specific action from the user, and the count is decreased. If no notifications are listed, when users open the For You tab, the page displays **You are all caught up!**

When users respond to a notification or deletes it, the notification is moved to the History folder. Users can view an archived message for 90 days, after which it is deleted.

By default, notifications are displayed with both the notification title and the message content. To display only the notification title, you can deactivate the **Display Push Notification Description** option in the Hub Services console.

Create Notifications in Workspace ONE Hub Services

You can use the notification builder in the Hub Services console to create a notification, select the target audience and create either an actionable notification or an informational notification.

Procedure

- 1 Navigate to the Hub Services Notifications page, click **New**, and then click **Create Notification**.
- 2 In the **Definition** page, define who receives the notification. Enter the name of the notification.
- 3 Select the **target audience**.

You can target customized notifications to specific audiences or send them to all employees in your organization. If you are authorized to send notifications to specific target audiences, the notification builder only displays those audience types for you to choose from.

The following are the available audience types that can be selected.

Audience Types	Description
All Employees	Notifications can be sent to all employees listed as users in the Workspace ONE Access service.
All Devices	Notifications can be sent to all devices configured in your Workspace ONE UEM environment, regardless of organization groups.

Audience Types	Description
Organization Group	Organization groups (OG) in the Workspace ONE UEM console are created to group individual organizations in your corporate structure, geographical location, business unit, or department. You can select a specific organization group in Workspace ONE UEM in which to send the notification.
Smart Group	Smart groups are customizable groups within Workspace ONE UEM that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision. You can select a smart group in Workspace ONE UEM in which to send the notification.
Platform	You can select a specific platform type to send a notification. The platforms are iOS, Android, macOS, and Windows.
Users Group	Groups in the Workspace ONE Access service are imported from your Active Directory or are created as local groups in the Workspace ONE Access console. You can select a group in Workspace ONE Access in which to send a notification.

- 4 If your organization implements the pre-hire onboarding process, to send the notification to the users in the pre-hire groups, select **Include Pre-hires**.
- 5 Select the priority of the notification.
 - **Standard**. Notifications are sent as standard by default.
 - **High- Priority**. Notifications that are sent high-priority are displayed at the top of the For You notifications page within the Priority section.
 - **Urgent**. Notifications that are sent as urgent are considered extremely important notifications that proactively alert users and require immediate attention or response.
- 6 Click **NEXT** to go to the **Content** page.
- 7 For Type, select the type of message you are creating, either **Actionable** or **Informational**.
 - Select **Actionable** to send a notification that requires your users to respond in the notification
 - Select **Informational** to send a notification that does not require the reader to take action on the notification.

8 In the **Content** section, complete the notification details.

Option	Description
Icon	<p>Use the default image, Intelligent Hub or add your company logo.</p> <p>The Image URL link can be to a JPG, PNG, or GIF file that is 96px by 96px. The file size cannot exceed 30 KB.</p> <p>If the URL link does not display, see How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom Tab on the Web Portal</p>
Title	<p>Enter the title that describe the notification topic</p> <p>The title displays in the notification heading.</p>
Subtitle (optional)	<p>The subtitle appears above the title.</p>
Media Type (optional)	<p>You can add either a video or an image to the notification card.</p> <p>To allow images and videos to display correctly in the notification banner, you must configure the web portal to permit cross-origin access to image or video files. The image or video HTML must provide a crossorigin attribute that in combination with an appropriate cross-origin resource sharing (CORS) header, allows images to display in the notification banner correctly. For more information about CORS, see the Cross-Origin Resources Sharing web site.</p> <p>To display images or videos correctly in the web portal, define the following CORS request headers on your website.</p> <pre data-bbox="644 982 1426 1054">Access-Control-Allow-Origin: <YOUR-HUB-APP-URL> Access-Control-Allow-Method: GET</pre> <p>To display an image in the notification banner, enter the full URL address that includes HTTPS. Example of a full image URL address, https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png. The image must be either a JPG or PNG file and the aspect ratio of the image is 4:3.</p> <p>To display a video in the notification banner, enter the full URL address that includes HTTPS that is displayed in the embedded code as the src value. For example, <code><source src="https://mozilla/media/videos/abcvideo.mp4"></code>.</p>
Description	<p>Type the notification message.</p>
Additional Details (optional)	<p>Click Add Details to add a feature, fact, or other item that you want to call out in the message. Enter as a label and the description.</p>
Links (optional)	<p>To add links to the notification, you add the link title that displays in the notification and then the complete link URL. Your notification can include up to 10 links.</p>
Attachments	<p>You can upload up to 10 files to attach with the notification. The individual file size cannot exceed 5 MB. Users can download or preview the attachments through a web browser.</p>

- 9 If you selected Actionable, configure the **Actions** section with the user's action and response flow.

Action and Response	Description
Action Button Text	Enter the text of the button that appears in the notification
Completed Action Button Text (optional)	Enter the text for the button that appears in the notification after the Completed action button is clicked.
Action Button Behavior	<p>Three action types can be selected.</p> <ul style="list-style-type: none"> ■ Open In. When you select the Open In action, you then enter the URL that opens when the button is clicked. You can also add a Hub deep link in your action notification to navigate users to a specific page in the app. In the Link text box, enter the URL. ■ API. When you select API, you then select the method to use to interact with the data being addressed in the notification. ■ API with User Input. When you select API with Parameters, in addition to selecting the method and API endpoint, you can add specific parameters and a value for the parameters. <p>For more information about parameters, go to the Workspace ONE Notification service API page. The Notifications Service reference guide is available from the Documentation tab.</p>
Make Action Repeatable	You can deactivate this option.
Primary	Enable Primary if you want Primary to be the first button in the For You notification bar.

You can create up to three actions in the notification.

For a list of URLs that you can use to deep link to Workspace ONE Intelligent Hub app pages for iOS devices, see [Chapter 13 Deep Links to Workspace ONE Intelligent Hub Pages Supported on iOS and Android Devices](#) .

- 10 Click **NEXT** to go to the **Scheduling** page to enable **Set Due Date** and set a date, time, and time zone by which the notification must be acted on.

Setting a due date is optional.

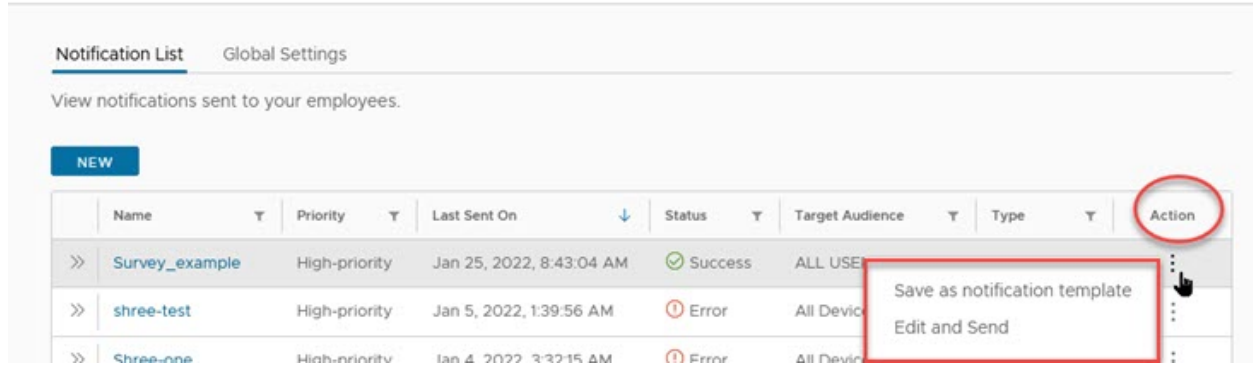
- 11 Click **NEXT** and in the **Summary** page review the notification details.

- 12 Click **CREATE** to create and send the notification.

Results

The notifications you create are available from the Notifications List table. In the Action column in the table, you can edit and resend a notification and you can make a notification into a notification template. See [Creating Notification Templates in Workspace ONE Hub Services](#).

Figure 8-2. Actions Available from the Notifications List



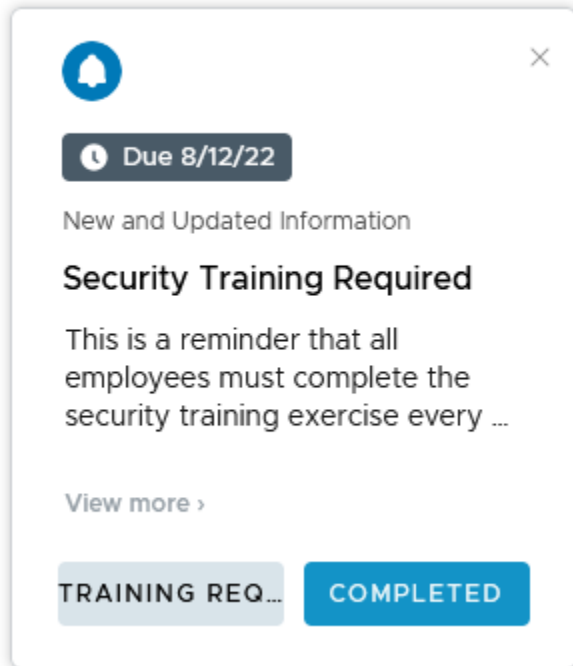
Example of How to Create Notifications in Workspace ONE Hub Services That Require Action

This example creates an actionable notification in Hub Services that asks the audience if they completed the required security training.

You can add a video or an image that displays in the notification. The notification can include up to 10 links and 10 attachments.

The notification includes two actionable options. Recipients that completed the training, click **Completed**. Recipients that have not completed the training, click **Training Required**. They are routed to the security training page.

Figure 8-3. Example of a Custom Notification



Procedure

- 1 Navigate to the Hub Services Notifications page and click **New** and then click **CREATE NOTIFICATION**.
- 2 Enter the name as **Security Training Required**.
This name displays in the status list on the Notifications page.
- 3 For **Target Audience Type**, select **All Employees**.
- 4 For **Priority**, because everyone must take this training and you do not want them to overlook the notification, select **High-priority**.
High-priority notifications display at the top of the notification list until the user acts on the notification.
- 5 Click **NEXT** to go to the Content page. Verify that the template is **Actionable**.
- 6 In the Content section, complete the notification details.

Option	Description
Icon	Use the default image, Intelligent Hub or you can add your own image for this notification.
Title	Enter the title as Security Training Required .
Subtitle (optional)	To highlight the completion date, enter the subtitle New and Updated Information .
Media Type (optional)	<p>You can add either a video or an image to the notification card.</p> <p>To allow images and videos to display correctly in the notification banner, you must configure the web portal to permit cross-origin access to image or video files. The HTML must provide a <code>crossorigin</code> attribute that in combination with an appropriate cross-origin resource sharing (CORS) header, allows images to display in the notification banner correctly. For more information about CORS, see the Cross-Origin Resources Sharing web site.</p> <p>To display images or videos correctly in the web portal, define the following CORS request headers on your website.</p> <pre>Access-Control-Allow-Origin: <YOUR-HUB-APP-URL> Access-Control-Allow-Method: GET</pre> <p>To display an image in the notification banner, enter the full URL address that includes <code>HTTPS</code>. Example of a full image URL address, <code>https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png</code>. The image must be either a JPG or PNG file and the aspect ratio of the image is 4:3.</p> <p>To display a video in the notification banner, enter the full URL address that includes <code>HTTPS</code> that is displayed in the embedded code as the <code>src</code> value. For example, <code><source src="https://mozilla/media/videos/abcvideo.mp4"></code>.</p>

Option	Description
Description	In this example, the message description reads as follows. This is a reminder that all employees must complete the security training exercise every year. If you already completed the training, click COMPLETED. If you have not completed the training, click TRAINING REQUIRED. The security training page will be displayed.
Additional Details (optional)	Click ADD Details to add a feature, fact, or other item that you want to call out in the message. Enter as a label and the description.
Links (optional)	Your notification can include up to 10 links.

7 This notification is created with two actions, **Completed** and **Training Required**.

- a The first action is for users who already completed the security training.

Option	Description
Action Button Text	Enter the text for the button that appears in the notification. Enter as COMPLETED .
Completed Action Button Text (optional)	Enter the text for the button that appears in the notification after the Completed action button is clicked. Enter as CONFIRMED .
Action Button Behavior	Select API as the button type.
Method	Select POST as the method. When users click COMPLETED , the answer is posted to the API endpoint URL.
API Endpoint	Enter the URL where the response is posted. For example, https://security-training-completed.acme.com .
Make Action Repeatable	Deactivate Make Action Repeatable .
Primary	Enable Primary . This button is the first button in the notification.

- b The second action is for users who have not completed the security training. When they click this button, they are sent to the security training URL.

Option	Description
Action Button Text	Enter the text for the button that appears in the notification. Enter as TRAINING REQUIRED .
Completed Action Button Text	Enter the text for the button that appears in the notification after Training Required is clicked. Enter as IN PROGRESS .
Action Button Type	Select Open In as the button type.
Link	Enter the link to the security training site. For example, enter https://security-training.example.com .
Repeatable	Deactivate Make Action Repeatable .
Primary	Deactivate Primary . This button appears after the button labeled Completed.

- c In the **Attachments** section, you can add up to 10 attachments to the notification. The individual file size cannot exceed 5 MB. Users can download or preview the attachments through a web browser.

8 Click **NEXT** to go to the **Scheduling** page to enable **Set Due Date** and set August 12, 2022 as the due date by which the notification must be acted on.

The due date displays in the notification.

9 Click **NEXT** to see a summary of the notification.

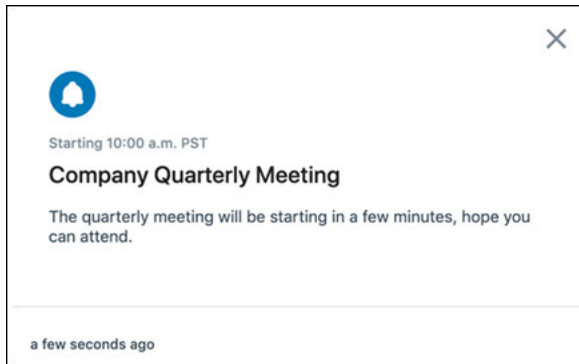
10 Click **CREATE** to create and send the notification.

Example of How to Create an Informational Notification in Workspace ONE Hub Services

Informational notifications do not require the user to take an action within the notification. Examples of the type of informational notification are system downtime, company-meeting reminders, or benefits-enrollment deadlines.

You can add a video or an image that displays in the notification. The notification can include up to 10 links and 10 attachments.

This example creates an information notification to remind users that the company all-hands meeting is starting soon.



Procedure

- 1 Navigate to the Hub Services Notifications page and click **New** and then click **Create Notification**.
- 2 Enter the name of the notification as **Company Quarterly Meeting Notification**.
This name displays in the status list on the Notifications page.
- 3 For the Target Audience Type, to send this notification out company wide, select **All Employees** and accept the default **Standard** priority.
- 4 Click **Next** to go to the Content page.
- 5 In the Template text-box drop-down menu, select **Informational**.
- 6 In the Content section, complete the notification details.

Option	Description
Icon	Use the default image, Intelligent Hub or add your company logo.
Title	Enter the title as Company Quarterly Meeting .
Subtitle (optional)	To highlight the meeting start time, enter the subtitle Starting at 10:00 a.m. PST .
Media Type (optional)	You can add either a video or an image to the notification card.
Description	Type the message. The quarterly meeting will be starting in a few minutes, hope you can attend.

Option	Description
Links (optional)	Your notification can include up to 10 links.
Additional Details	Click Add Details to add a feature, fact, or other item that you want to call out in the notification. Enter as a label and the description.
Attachments	You can upload up to 10 files to attach with the notification. The individual file size cannot exceed 5 MB. Users can download or preview the attachments through a web browser.

- 7 Click **Next** to see a summary of the notification.
- 8 Click **Create** to create and send the notification.

Action Methods That You Can Configure in the Workspace ONE Notifications API

Besides the action methods you can configure in the Hub Services Custom Notification wizard, you can configure additional action methods when you use the Notification Services API to create notifications.

To see code examples for these action notifications, go to the documentation tab on the Workspace ONE Notifications Service API page, <https://code.vmware.com/apis/402#/Notifications>.

- “action_key”:”OPEN_IN”. Make an API call to open a specific URL in the system’s default browser. For example, create a change password notification that includes the change password action with a link to the password change URL.
- “action_key”:”DIRECT”. Make an API call to the specific URL where the type value is the HTTP method, and the request value contains hard coded fields that are sent as payload when the API call runs. For example, create a survey question that requires a Yes or No answer. When a user clicks to answer the questions, the response, either Yes or NO, is sent to the URL listed.
- “action_key”:”USER_INPUT”. Make an API call to a specific URL where the type value is the HTTP method where the user enters some input that is sent with the payload. For example, create an Accept or Deny notification where the recipient is required to add a comment when denying the request. This response is sent as the payload of the API call to the specified URL.

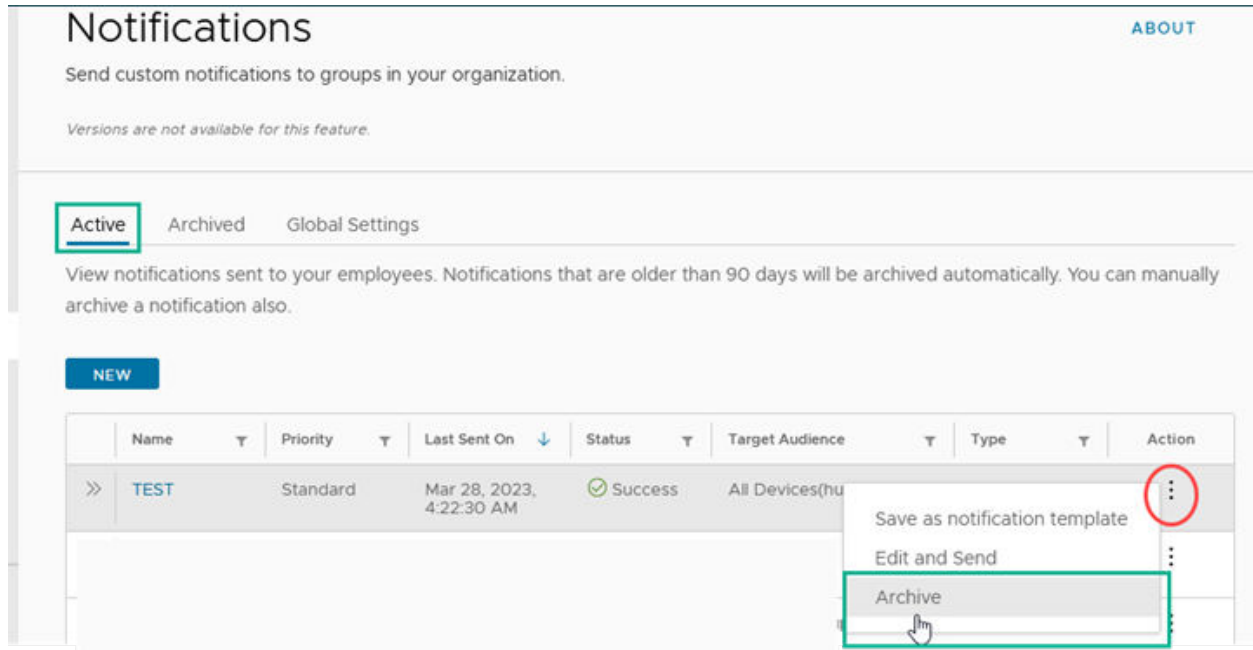
When using DIRECT or USER_INPUT as the action type, make sure that the URL you use does not require authentication to access. If an authorization token is required, the API call fails. See the Notification Service API documentation for examples of the API code to use.

Archiving Notifications (Cloud only)

To maintain the Notification list with only active notifications, notifications that are over 90 days old are automatically moved to the **Notifications > Archived** tab in the Hub services console. In

addition, Hub Services super admins can move individual notifications that are less than 90 days old from the active notification list to the archived list.

Only super admins can access the Archived list page and can archive notifications. Users with other admin roles do not see the **Notifications > Archived** tab in their view of the Hub Services console.



Notifications ABOUT

Send custom notifications to groups in your organization.

Versions are not available for this feature.

Active Archived Global Settings

View notifications sent to your employees. Notifications that are older than 90 days will be archived automatically. You can manually archive a notification also.

NEW

Name	Priority	Last Sent On	Status	Target Audience	Type	Action
>> TEST	Standard	Mar 28, 2023, 4:22:30 AM	Success	All Devices(hu		<ul style="list-style-type: none">Save as notification templateEdit and SendArchive

Archived notifications cannot be moved back to the notifications list, but in the archived list, super admins can select a notification to save as a template or to edit and send. Depending on the selection, either the template configuration page or the notification builder page is displayed.

Notifications

[ABOUT](#)

Send custom notifications to groups in your organization.

Versions are not available for this feature.

Active **Archived** Global Settings

All notifications that are older than 90 days will be moved here automatically. Notifications manually archived by admins will be available here as well.

Name	Priority	Last Sent On	Status	Target Audience	Type	Action
>> test	Sticky	Mar 2, 2023, 7:43:36 PM	Success	ALL USERS	Sticky	⋮
>> test	Standard	Feb 16, 2023, 8:17:16 AM	Success	ALL US		⋮

Save as notification template
Edit and Send

Manage Columns

1 - 5 of 5 Notifications

Note Archiving a notification does not remove it from the user's **For You** tab in the Workspace ONE Intelligent Hub app or Hub portal. Users can view messages in History for 90 days, after which the notification is deleted from their device.

Creating Notification Templates in Workspace ONE Hub Services

You can create notification templates that you can use to create custom notifications quickly. Using a notification template let you standardize the message format for notifications. Notification templates that you save are listed on the Notification template page. You can edit and delete notification templates.

When you select a notification template to use, you can customize the content, select the target audience, and set the notification priority. When you send the notification, the customized notification is added to the list of notifications sent on the Notifications page. The template is not changed.

For more information about notifications, see [Chapter 8 Using Hub Notifications Service in Workspace ONE Hub Services](#).

Create a Notification Template

You can create a new notification template or you can save an existing notification as a notification template.

- 1 To create a notification template, navigate to the Hub Services Notifications page, click **New** and then click **Create Template**.

To create a notification from a notification in the Notification list, in the **Action** column of the notification, click the three dots menu and select **Save as notification template**.

- 2 Enter the name and a description of the template. Click **NEXT**.
- 3 In the **Content** page, select the type of notification, **Actionable** or **Informational** and set up the content of the notification.
 - Select **Actionable** to send a notification that requires your users to respond in the notification
 - Select **Informational** to send a notification that does not require the reader to take action on the notification.

If you selected to save a notification as a template, the Content page is configured. You can edit the page.

- a Configure the content of the message.

Option	Description
Icon	By default, the Workspace ONE Intelligent Hub icon default image displays in the notification. You can upload an image file or enter a URL link to the image. Upload JPG, PNG, or GIF file that is 40px by 40px for best results. The file size cannot exceed 30 KB. The Image URL link can be to a JPG, PNG, or GIF file that is 96px by 96px. The file size cannot exceed 30 KB. If the URL link does not display, see How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom Tab on the Web Portal
Title	Enter a title that describes the notification topic
Subtitle	Optional. The subtitle appears above the title.

Option	Description
Media Type (optional)	<p>You can add either a video or an image to the notification card.</p> <p>To allow images and videos to display correctly in the notification banner, you must configure the web portal to permit cross-origin access to image or video files. The HTML must provide a <code>crossorigin</code> attribute that in combination with an appropriate cross-origin resource sharing (CORS) header, allows images to display in the notification banner correctly. For more information about CORS, see the Cross-Origin Resources Sharing web site.</p> <p>To display images or videos correctly in the web portal, define the following CORS request headers on your website.</p> <pre>Access-Control-Allow-Origin: <YOUR-HUB-APP-URL> Access-Control-Allow-Method: GET</pre> <p>To display an image in the notification banner, enter the full URL address that includes <code>HTTPS</code>. Example of a full image URL address, <code>https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png</code>. The image must be either a JPG or PNG file and the aspect ratio of the image is 4:3.</p> <p>To display a video in the notification banner, enter the full URL address that includes <code>HTTPS</code> that is displayed in the embedded code as the <code>src</code> value. For example, <code><source src="https://mozilla/media/videos/abcvideo.mp4"></code>.</p>
Description	Type the notification message in the Description box.
Additional Details	Click Add Details to add a feature, fact, or other item that you want to call out in the message. Enter as a label and the description.
Links (optional)	Add the link title that displays in the notification and add the complete link URL. The notification can include up to 10 links.

- b If you select **Actionable**, configure the Actions section with the user's action and response flow .

Three action types can be selected.

- **Open In.** When you select the Open In action, you then enter the URL that opens when the button is clicked.
- **API.** When you select API, you then select the method to use to interact with the data being addressed in the notification. See
- **API with Parameters.** When you select API with Parameters, in addition to selecting the method and API endpoint, you can add specific parameters and a value for the parameters.

For more information about parameters, go to the Workspace ONE Notification service API page. The Notifications Service reference guide is available from the Documentation tab.

Up to three actions can be created.

- c In the **Attachments** section, you can add up to 10 attachments to the notification template. The individual file size cannot exceed 5 MB.
- 4 Click **NEXT** and then **SAVE**.

The notification template is saved to the Notification Template list.

Use Notification Templates to Create and Send Notifications

You can

- 1 Navigate to the Hub Services Notifications page, Click **NEW** to open the page to the Notification Template list.
- 2 In the **Action** column for the notification template to use, click **USE**.
- 3 In the Custom Notification Definition page, enter a name for the notification, select the target audience and set the priority.

Click **NEXT**.

- 4 Review the configuration in the **Content** page and make required changes. Click **NEXT** to see a summary of the notification information.

Note Changes you make to the Content page do not change the notification template.

- 5 Click **CREATE**.

The notification is sent and it is added to the **Notification List** on the Notifications page.

Setting Up Push Notifications in Hub Services for Workspace ONE Access (On Premises only)

To use the push notification feature in the Hub Services Notifications service with on premises Workspace ONE Access deployments, you must register Workspace ONE Access to the cloud notifications service.

To register Workspace ONE Access, you copy the token from VMware `my.workspaceone.com`, and paste the token in the Notifications Global Settings page in the Hub Services console to generate the certificate.

Procedure to get the Token

- 1 Log in to the VMware My Workspace ONE portal, <https://my.workspaceone.com>,
- 2 Navigate to <https://my.workspaceone.com/mycompany/certificates/awinstall/authtoken>.

The Generate A Token page displays your token in the Your Token section.

- 3 In the **Your Token** section, click **COPY TO CLIPBOARD**.

Save the copied token to add to the Notifications page in the Hub Services console.

Add the Token to Hub Services and Generate the Certificate

- 1 Navigate to the Hub Services console **Home** page.
- 2 Click **Notifications > Global Settings**.
- 3 In the **Push Notifications** section, paste the Workspace ONE Access token that you copied.
- 4 Click **GENERATE**.

The push notification certificate is generated and the page is updated to show that the certificate is active.

- 5 If you want to display only the title of the notification to users, deactivate the **Display Push Notification** option. Otherwise both the notification title and the message content are displayed.
- 6 Click **Save**.

The Workspace ONE Access on premises service is registered to the cloud notifications service.

The certificate token is good for three years. Make sure you renew the certificate to maintain uninterrupted push notifications.

Integrate Hub Services with Workspace ONE Intelligence to Provide Notification Analytics and Automation Workflows

To collect engagement analytics about how users interact with notification that you send through Hub Services, you can integrate with VMware Workspace ONE[®] Intelligence[™].

Workspace ONE Intelligence is a cloud service built for the Workspace ONE platform that provides analytics and automation for your digital workspace.

About Notification Analytics

When you integrate Hub Services with Workspace ONE Intelligence, you can collect analytics about how users interact with notifications in the Workspace ONE Intelligent Hub app.

In the Workspace ONE Intelligence console you can import dashboard samples to customize or you can create your own dashboard to display the analytics data for notifications created in Hub Services. Download Hub Notification analytics dashboard code samples from the [VMware Sample Exchange site](#).

In the dashboard, you can collect analytics for the following types of user events.

- **Action.** The system logs when users successfully complete the action requested in the notification.
- **Created.** The system logs the number of notifications that admins created.
- **Dismiss.** The system logs when users select the **X** in the top right corner of the card to delete the notification and send it to the history file.
- **Open.** The system logs when users open a notification to see the details in the message.

- Sent. The system logs the number of notifications the system sends to users or devices.
- Viewed. The system logs when a notification displays on a user's **For You** tab.

You can find integration and configuration details in the *VMware Workspace ONE Intelligence Products* guide. To set up analytics dashboard for notifications, see the [VMware Workspace ONE Hub Services Integration](#) section.

About Notification Workflows in Workspace ONE Intelligence

In Workspace ONE Intelligence, you can also use automation workflows to target and send Hub notifications to devices about apps, devices, remediation resources, and other types of updates. These notifications appear in the **For You** tab in the Workspace ONE Intelligent Hub app.

You can find details about setting up automation workflows in the *VMware Workspace ONE Intelligence Products* guide [Automations for Workspace ONE Intelligence, Configure workflows](#) section.

Enabling Access to People Search in the Workspace ONE Intelligent Hub App

9

When you fully integrate Hub Services with Workspace ONE Access, in the Hub Services console, you can enable access to the People service to let users search for their colleagues and view user details and organizational hierarchy directly from the Workspace ONE Intelligent Hub app or the Hub portal.

To use the People service in the Workspace ONE Intelligent Hub app, you enable the People feature in the Hub Services console. In the Workspace ONE Access console, you configure the directory to use for People Search, and you map the Active Directory title, managerDN, and distinguishedName attributes to the Workspace ONE Access user attributes.

The organizational hierarchy and direct reports information in the People Search results is based on the managerDN attribute. To display user photos, you map the Active Directory attribute thumbnailPhoto to the imageURL attribute in the Workspace ONE Access directory. These attributes become the user profile information that displays in People search results.

Note This feature is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

In the Hub Services console, you manage the information that is available in the user's profile displayed in the People tab. You can select which user attributes to include in the profile description, change the user attribute names to something more friendly, and arrange the order in which the attributes are displayed in the user profile page.

When you enable access to the People service, the People tab displays in the Workspace ONE Intelligent Hub app and the Hub portal along with the other tabs.

Users can search for people by first name, last name, and email address. Based on the attributes that are mapped to the directory, the following can be viewed.

- User profile details
- User profile picture
- Organization hierarchy of the user

From the user profile page, users can immediately email, call, or text the user.

For configuration information from the Workspace ONE Access console, see [Set Up People Search in Workspace ONE Access](#).

Read the following topics next:

- [Enable People Service in Hub Services](#)

Enable People Service in Hub Services

When you enable the People service in the Hub Services console, users in your organization can search in the Workspace ONE Intelligent Hub app or Hub portal for their colleagues and view users' details and organization charts.

Prerequisites

Note This feature is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

- Workspace ONE UEM services and Workspace ONE Access services integrated for single sign-on and identity management.
- Workspace ONE Access configured as the authentication method in the Workspace ONE UEM console.
- Active Directory integrated with Workspace ONE Access.
- People Search configured in the Workspace ONE Access console.

Procedure

- 1 Navigate to the Hub Services console Home page.
- 2 Click **People** and toggle **Enable People** to green.
- 3 If custom attributes are displayed on the page, select the attributes you want to display in the user profile.
 - a In the **Available Attributes** section, enable the attributes you want to use. They are added to the Enabled Attributes section.
 - b In the **Enabled Attributes** section, you can change the attribute name. In the **Display Name** column, enter the name to display in the user profile.
 - c You can also arrange the order that the custom attributes display in the user profile. In the **Order** column, select the order number from the drop-down menu.

Custom Attributes

Configure custom attributes setup in WS1 Access. Enabled attributes will appear under an employee's profile.

Enabled Attributes

Order	Attribute	Display Name	
1 ▾	customAttr	Sr. Manager	<input checked="" type="checkbox"/>

4 Click **SAVE**.

Results

The People tab is added to the Workspace ONE Intelligent Hub app, the Hub portal view in browsers, and desktop views. Users in your organization can search for their colleagues and view users' details and organization charts.

Note If the People tab does not display after you enable the People feature, you can push the changes. Before you run this command to push the change, make sure that you are logged into the Hub portal. Open a new tab and enter this URL, substituting your domain name for myco.example.com. **`https://<myco.example.com>/catalog-portal/services/api/featureCustomizations?refreshCache=true`**.

Configuring Workspace ONE Intelligent Hub Employee Self-Service Features in Hub Services

10

In the Hub Services console Employee Self-Service page, you can customize the type of self-service support that is available in Workspace ONE Intelligent Hub.

You can add helpful links to the self-service tab to empower and educate users about how to perform basic device management tasks, investigate issues, and fix problems. These links can reduce the number of help desk tickets and support issues. Some of the non-critical actions users can take include clearing their passcode, make noise, or lock their device.

You can create different versions of the employee self-service tab and design helpful links for specific groups of users.

For global settings, the option to view the self-service tab in the browser is on by default. You can turn off this option in the Employee Self-Service page. You can create versions of the employee self-service tab and design the helpful links for specific groups of users and add a version in the Hub template assigned to a specific group.

Figure 10-1. Employee Self-Service Page in Hub Services Console

Employee Self-Service

Configure a self-service tab for employees to access helpful links and manage their devices.

VERSION: GLOBAL ▾

Global Settings

These default settings will be used by Intelligent Hub unless overridden by a template assignment.

Define whether to enable the self-service tab by default in Intelligent Hub

Enable Employee Self-Service

Tab Name Support

Configurations

Configure device self-service and helpful links for employees.

Device Self-Service

Allows employees to monitor and manage their own devices with.

Add Device	<input checked="" type="checkbox"/> Enabled
Install profiles	<input checked="" type="checkbox"/> Enabled
Encryption Recovery Key	<input checked="" type="checkbox"/> Enabled
Critical Actions	<input type="checkbox"/> Disabled
Non Critical Actions	<input checked="" type="checkbox"/> Enabled

[EDIT](#)

Helpful Links

Allow employees to troubleshoot issues by adding quick links to how-to-guides and other resources.

Links **1**

[EDIT](#)

Customize the Employee Self-Service Tab Label

The tab name that appears in the Workspace ONE Intelligent Hub app is labeled **Support**. You can modify this label in the Hub console **Employee Self-Service** page. When you change the label, users see the updated name in the navigation bar when they refresh the Workspace ONE Intelligent Hub app view.

Setting Up User's Device Self-Service Options

When Device Self-Service is configured, users monitor and manage their own devices from Workspace ONE Intelligent Hub. Users go to the **My Devices** section of the Support tab to see which devices are managed from the Workspace ONE Intelligent Hub, and users can add other devices.

In the Device Self-Service section, you configure the following user device management options.

Feature to enable	Description
Add Device	<p>Users can register a new device through email, SMS, or a QR code.</p> <p>Users can see the status of their devices and they can click Sync Device to sync their profiles to the device.</p>
Install Profiles	<p>Users can view and install optional profiles or reinstall automatic profiles.</p> <p>Users can see their work apps and devices that are installed, and they can click Reinstall.</p>
Encryption Recovery Key	<p>The encryption recovery key is a unique numerical password that users can use to regain access to their macOS or Windows device.</p> <p>When this option is enabled, users can retrieve their desktop encryption recovery keys for their enrolled and encrypted macOS and Windows devices from the Workspace ONE Intelligent Hub Support tab, instead of submitting a support ticket requesting a recovery key.</p>
Critical Actions	<p>When the Critical Actions setting is enabled, users can view and take self-service actions to delete a device and to enterprise wipe a device to unenroll and remove all managed enterprise resources from the selected device.</p>
Non Critical Actions	<p>The Non Critical Actions setting is enabled by default. In the Workspace ONE Intelligent Hub Support tab, users can take self-service actions to change their passcode, enable the Make Noise setting to hear Noise notification alert on their device, or lock their device.</p>

Add Helpful Links

In the Helpful Links section, you can add links to promote and direct users to internal or external sites and knowledge base articles for self-service help. These links can give users a chance to look for solutions to issues before they reach out to your support service. Users can find these links in the Workspace ONE Intelligent Hub Support tab, **Helpful Resources** section.

You can use `wsonithub://{deeplink}` as a valid URL to set up helpful links that take users to other pages in the Workspace ONE Intelligent Hub app.

You can use `awb(s)://{URL}` as a valid URL to launch web pages in a web app from Workspace ONE Intelligent Hub.

You can add up to 10 links to direct users to resources. Users can find these links in the Workspace ONE Intelligent Hub Support tab, **Helpful links** section.

Helpful Links
Add up to 10 links that will direct employees to how-to guides and other resources to help them troubleshoot issues on their own.

	Title	Link
1	<u>VMware</u>	<u>https://www.vmware.com/</u>
2	<u>Google Weblink</u>	<u>awbs://google.com</u> <small>Non-http(s) URLs may not work properly on all platforms. Use Templates to set up helpful links by platform.</small>
3	<u>Deeplink to Hub</u>	<u>wsonehub://go.to.hub</u> <small>Non-http(s) URLs may not work properly on all platforms. Use Templates to set up helpful links by platform.</small>

[ADD SECTION](#)

Manage Contact Information

When Workspace ONE UEM is configured to enroll devices and is configured with Hub Services, a Contacts section displays in the Employee Self-Service page. The support email and phone number that display are configured in the Workspace ONE UEM console **Device > Device Settings > Device & Users > General > Enrollment > Customization** tab.

Note The Customization tab shows an example email and phone numbers. If you do not change the example settings in the Workspace ONE UEM console, this example information displays in the Contacts section. See [Configure Contact Email and Phone Number Information for Workspace ONE Intelligent Hub Support Tab](#).

Read the following topics next:

- [Setting Up Self-Service Quick Actions in the Support Tab \(Cloud only\)](#)

Setting Up Self-Service Quick Actions in the Support Tab (Cloud only)

You can create links in the Workspace ONE Intelligent Hub app's Support tab as Quick Actions links to access Workspace ONE UEM Freestyle Orchestrator workflows. These Quick Actions in the Support tab help users easily find and execute workflows for problem-solving or configuring their digital workspace.

You use the Freestyle Orchestrator feature in the Workspace ONE UEM console to create customized workflows to automate endpoint configurations on Windows devices. In Freestyle, you configure a workflow, assign the workflow to the Windows platform, and select a smart group that can access the workflow. When Workspace ONE UEM is configured with Hub Services, in the Workspace ONE UEM console select **Show in Hub** to deploy the workflow to the Hub catalog when the workflow is published.

To set up these workflows as quick actions, you configure Hub Services global or custom templates to list workflows as Quick Actions in the Workspace ONE Intelligent Hub Support tab. When you make them available in the Support tab, users can easily find and access helpful quick actions for their supported device.

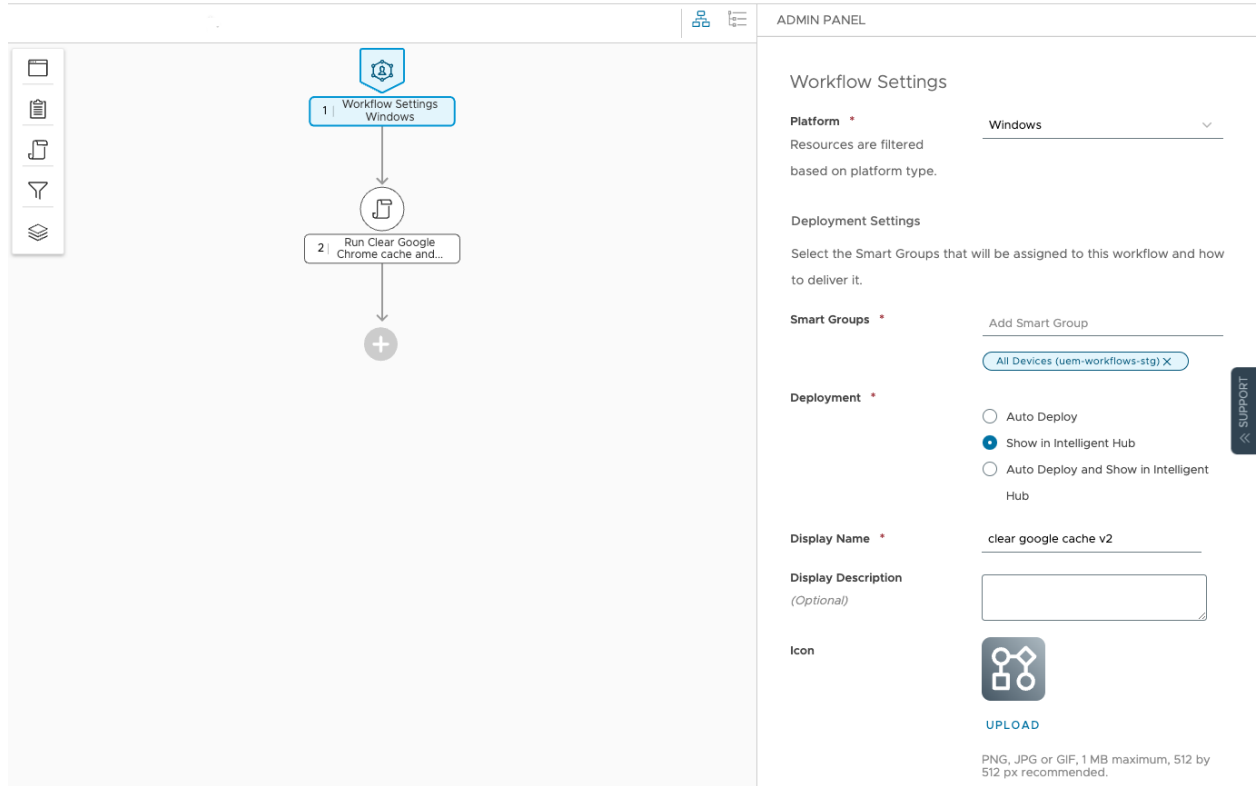
Prerequisites

- Platform support for Windows 10 with Workspace ONE Intelligent Hub app 23.08 or later

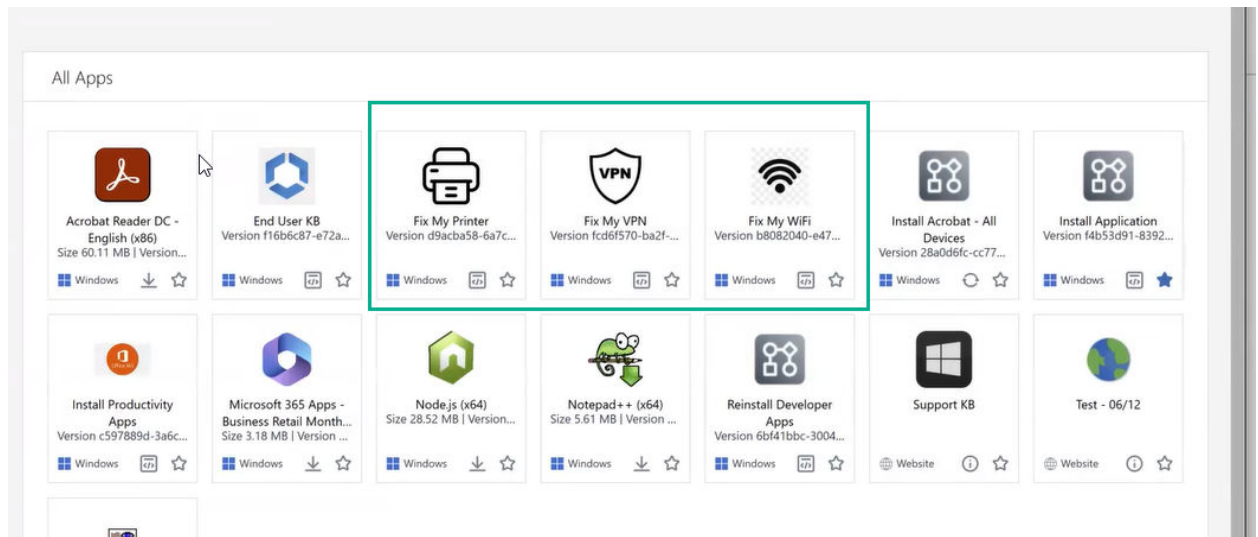
Overview of Using Freestyle Orchestrator to Create Workflows for Workspace ONE Intelligent Hub App Catalog

The following outlines the high-level steps in the Workspace ONE UEM console to create workflows that displays in the Hub app catalog and then can be configured as quick actions that display in the device Support tab. See the [Freestyle Orchestrator guide](#) for detailed steps about creating and managing workflows.

- 1 In the Workspace ONE UEM console > Freestyle > Freestyle Orchestrator page, create a workflow.
- 2 In the **Admin Panel**, select the Windows platform and select the smart groups to which you want to assign the workflow.
- 3 In the **Admin Panel**, configure the Deployment setting **Show in Intelligent Hub**. When the workflows are published in the Workspace ONE UEM console, the workflows are displayed in the Workspace ONE Intelligent Hub Apps catalog. To make the quick action links easier to find, In the Hub Services console you can set up these workflows as quick actions that display in the Workspace ONE Intelligent Hub Support tab on devices.



When the workflow is published in Workspace ONE UEM, the workflow displays in the Hub app catalog.



Configure Hub Services Templates to Display Workflows as Quick Actions on Devices

You can edit the Hub Services global and custom templates to add quick actions. You can also create custom templates and add quick actions in the employee self-service tab that are specific to the users in the smart groups that are assigned to that template.

Example use case where you edit both global and custom templates to add quick actions for different users

- The global template is assigned to the All Devices smart group. In the Employee Self-Service page, you edit the Global template to add quick actions that is applicable to all devices, such as a quick action link to the Fix My Printer workflow.

When any user logs into Workspace ONE Intelligent Hub with a Windows device that is registered within the All Devices smart group in the Global template, they see the Fix My Printer quick action for the Windows device they are currently using.

- In an Engineering Group custom template that is assigned to the Engineering smart group, you edit the template to add quick actions that are applicable to only devices registered in the Engineering Group, such as a quick action for adding Engineering Pager Duty notification.

When engineers that belong to the Engineering group log into the Workspace ONE Intelligent Hub , they see the Install Engineering Pager Duty quick action assigned to their smart group and device type.

For more information about how to set up templates in the Hub Services console, see [Chapter 5 Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users](#) .

Procedure

- 1 Navigate to the Hub Services console Home page and click **Employee Self-Service**.
- 2 Either select the GLOBAL template to edit or create or edit a customized template.

Workspace ONE Hub Services

Home
Templates
App Catalog
Branding
Custom Tab

1 Employee Self-Service
Notifications
People
New Hire Welcome
Shift-Based Access Control
System Settings

ADMIN CONFIGURATIONS
Admin Roles

Employee Self-Service

Configure a self-service tab for employees to access helpful links and resources.

VERSION: GLOBAL **2**

- Global
- Engineering Group - Template
- pm_group
- qa_ssakshi

[ADD VERSION](#)

Enable Employee Self-Service

Tab Name Support

Configurations

Configure device self-service and helpful links for employees.

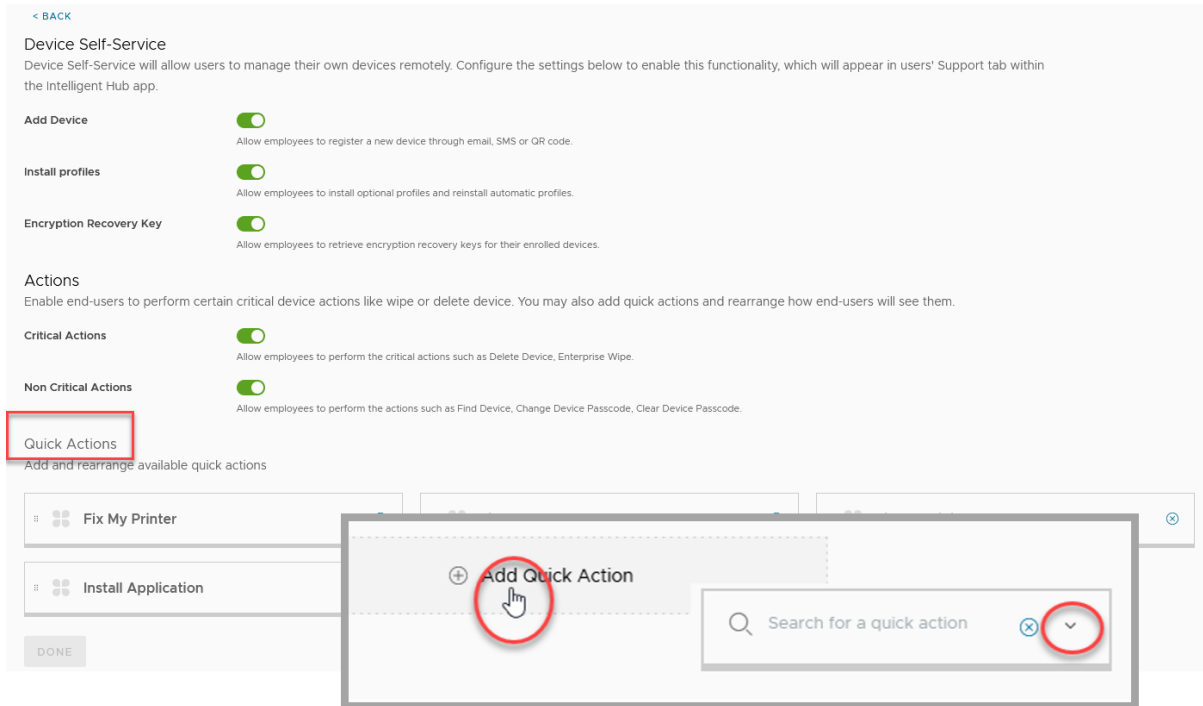
Device Self-Service

Allows employees to monitor and manage their own devices with.

Add Device	<input checked="" type="checkbox"/> Enabled
Install profiles	<input checked="" type="checkbox"/> Enabled
Encryption Recovery Key	<input checked="" type="checkbox"/> Enabled
Critical Actions	<input checked="" type="checkbox"/> Enabled
Non Critical Actions	<input checked="" type="checkbox"/> Enabled

3 [EDIT](#)

- 3 In the **Device Self-Service** pane, click **EDIT**.
- 4 In the **Quick Actions** section, click **Add Quick Action** to open the search box.



- 5 In the **Search for a quick action** search box, the workflows that are in the Workspace ONE Intelligent Hub app catalog are listed in the drop-down menu. Start typing the workflow name or click the arrow to select an available workflow to add as quick actions.

Repeat step 4 to add additional quick actions to the template.

- 6 Click **DONE**.

Using Hub Services Shift-Based Access Control to Manage Shift-Based Workers Access to Resources in Workspace ONE Intelligent Hub App

11

You can enable the Shift-based Access Control feature in the Hub Services console and set up a shift-based access control system within VMware Workspace ONE Intelligent Hub to selectively restrict when frontline workers can access their work content, services, and apps if they are not currently working on a shift.

Note Shift-based access control is available now as a Limited Availability release. reach out to your account team for the steps required to enable Shift-based Access Control with the UKG Dimensions feature.

Shift-based Access Control works with the third-party timekeeping system UKG Dimensions You configure the settings for your UKG Dimensions timekeeping system in the Hub Services console. This allows you to dynamically retrieve real-time data about the employee's working status from the UKG Dimensions Timekeeping system.

You configure Hub Services templates to restrict access to the Custom tab, People tab, Notification For You tab to pause notifications, and Employee Self-Service tab in the Workspace ONE Intelligent Hub app and Hub portal.

In the Workspace ONE UEM console, you configure the Time Awareness component profile and assign the profile to the Workspace ONE Intelligent Hub app if you do not want your workers to access the Workspace ONE Intelligent Hub app from their iOS and Android mobile devices when they are not working.

In the Workspace ONE Access console, you configure a shift-based access authorization method and create application-specific access policies to manage when workers can access web and desktop apps from your company's application catalog.

You configure Workspace ONE Access to be the source of authentication when users access their resources from the Workspace ONE Intelligent Hub app or Hub portal.

See the [Configure VMware Workspace ONE Shift-Based Access Control with UKG Dimensions Time Keeping System](#) guide for how to set up shift-based access control for Workspace ONE.

About MDM Enrollment in Workspace ONE Intelligent Hub

12

The Workspace ONE Intelligent Hub enrollment process secures a connection between devices and the Workspace ONE UEM environment. The Workspace ONE Intelligent Hub app facilitates enrollment and allows for real-time management and access to device information.

To enroll devices using the Workspace ONE Intelligent Hub, you can ask your users to download the Workspace ONE Intelligent Hub app from the appropriate app store. When users download the app, they can (depending on the configuration) either enter their email address, the server URL and group ID, or use the QR code reader to start the enrollment using Workspace ONE Intelligent Hub.

For documentation about mobile device management, including how to enroll devices, create profiles to manage compliance, and manage devices through the Workspace ONE UEM console, see the specific device management guide on the [Workspace ONE UEM](#) documentation landing page.

Read the following topics next:

- [Workspace ONE Intelligent Hub App Mobile Device Management Settings](#)
- [Enable Intelligent Hub Device Enrollment and Authentication Mode](#)
- [Enable Unmanaged Enrollment for iOS Devices](#)
- [Configure Contact Email and Phone Number Information for Workspace ONE Intelligent Hub Support Tab](#)
- [Workspace ONE UEM Device Management Options for Public and Internal Apps](#)
- [Managing Access to Applications in Workspace ONE UEM](#)
- [Configuring Mobile Single Sign-On from Workspace ONE UEM Enrolled Devices](#)

Workspace ONE Intelligent Hub App Mobile Device Management Settings

The Workspace ONE Intelligent Hub mobile device management feature facilitates enrollment and allows for real-time management and access to relevant device information.

The Workspace ONE Intelligent Hub app facilitates MDM enrollment in the traditional MDM uses cases for Workspace ONE UEM on premises and SaaS deployments. You configure the Workspace ONE Intelligent Hub MDM settings for each of the platforms from the Workspace ONE UEM console Device & Users > <Devicetype> Intelligent Hub Settings page.

You can configure end-user support email and phone number as contact information in the Workspace ONE UEM admin console Device Settings > Devices & Users > General > Enrollment > Customization tab. This information is displayed in the Workspace ONE Intelligent Hub employee self-service tab on devices and in the Hub portal.

The Workspace ONE Intelligent Hub app runs in device management mode. When users initially launch the Workspace ONE Intelligent Hub app, they enter their corporate credentials to self-activate their devices.

The following is an overview of the Workspace ONE Intelligent Hub settings that can be configured for device management. The exact settings you can configure vary depending on the platform. For information about configuring Workspace ONE Intelligent Hub for device management, see the specific platform guide in the Productivity Apps Documentation section in the [Workspace ONE UEM Documentation](#) center.

Table 12-1. Workspace ONE Intelligent Hub Settings Descriptions

Section Name	Setting	Description
General		
	Disable Unenroll Option in Intelligent Hub.	This setting allows or blocks the ability for a user to unenroll from the Workspace ONE Intelligent Hub. When this box is selected, the unenroll option is deactivated. The setting label is changed to Reenroll , to allow the user to enroll the device to another user but not be able to remove the MDM profile.
	Background App Refresh	This setting enables the Workspace ONE Intelligent Hub to send its beacon data sample to the UEM console when it is running in the background on an iOS device. This sample is sent during the interval specified in the Minimum Refresh Interval setting.
	Minimum Refresh Interval	This drop-down setting sets the minimum interval for the Intelligent Hub to send its beacon data sample. For example, if this setting is set to 4 hours (default), then a sample is sent to the UEM console if a beacon sample was not sent in the last 4 hours.
	Transmit on Wi-Fi only	This setting requires that any samples or communication must take place over Wi-Fi only and not a cellular network.
Area		
	Collect Location Data	This setting enables the Workspace ONE Intelligent Hub to request permission from the user to track location data. If the user allows this permission, the Intelligent Hub sends location coordinates back in its beacon sample.

Table 12-1. Workspace ONE Intelligent Hub Settings Descriptions (continued)

Section Name	Setting	Description
	Detect iBeacon Area	This setting enables the Workspace ONE Intelligent Hub to check for iBeacon devices in its surrounding area and display the devices in the Intelligent Hub.
Telecom		
	Collect Cellular Data Usage	This setting enables the Workspace ONE Intelligent Hub to collect the cellular data usage from the device and display the information in the Intelligent Hub.
Self Service Setting		
	Self Service Enabled	This setting enables the Workspace ONE Intelligent Hub to display the compliance policies assigned to the device and the user, to monitor and refresh the status of each policy. If enabled, users can see if their devices are compliant.
SDK Profile		
	SKD Profile (Legacy)	This drop-down setting is a deprecated field for selecting which SDK settings to deploy to the Workspace ONE Intelligent Hub to configure settings like PIN Code, Analytics, and Branding.
	SDK Profile V2	This drop-down setting is the active field for selecting which SDK settings to deploy to the Workspace ONE Intelligent Hub to configure settings like PIN code, analytics, and custom branding for the Workspace ONE Intelligent Hub and more.

Enable Intelligent Hub Device Enrollment and Authentication Mode

You select the authentication mode and enable direct device enrollment for the Workspace ONE Intelligent Hub app from the Workspace ONE UEM console **Devices & Users > General > Enrollment > Authentication** page.

The authentication mode is Workspace ONE UEM when you are using the Workspace ONE Intelligent Hub app without integrating with Workspace ONE Access. Select Workspace ONE Access when Hub Services is configured to use the integrated Workspace ONE Access service for authentication.

Procedure

- 1 In the Workspace ONE UEM console, select your **Global > customer-level organization group** and navigate to the **Devices > Devices Settings > Devices & Users > General > Enrollment** page.
- 2 In the Authentication tab, **Current Settings** section, select **Override**.

- 3 To integrate fully with Workspace ONE Access, in the **Source of Authentication for Intelligent Hub**, select **Identity Manager**.
- 4 For direct device enrollment from the Workspace ONE Intelligent Hub app on devices, enable **Require Intelligent Hub Enrollment for iOS**, **Require Intelligent Hub Enrollment for macOS**, and **Require Intelligent Hub Enrollment for Android**.
- 5 Click **Save**.

Enable Unmanaged Enrollment for iOS Devices

Devices enrolled through the Workspace ONE Intelligent Hub app are MDM managed by default. To allow some iOS devices to enroll without MDM management you must enable the unmanaged mode for a smart group.

The selection criteria available is OS version, ownership type, and user group.

In unmanaged enrollment, users can access applications that require a basic level of security. When users try to access an app that requires management, users are guided through the MDM enrollment process. You use the adaptive management app policies to control device management levels for iOS devices enrolled without management.

Procedure

- 1 In the Workspace ONE UEM console, select the organization group to be enabled with unmanaged enrollment and navigate to the **Devices > Devices Settings > Devices & Users > General > Enrollment > Management Mode** page.
- 2 In **Current Settings**, click **Override**.
- 3 For iOS, select **Enabled**.
- 4 In **Smart Groups**, add the smart group that is enabled for unmanaged enrollments.
- 5 Click **Save**.

Results

Users with iOS devices from the configured smart group are entitled unmanaged access to apps. Users can use the Workspace ONE Intelligent Hub app to access applications that require a basic level of security without the device being enrolled into Workspace ONE UEM Mobile Device Management.

What to do next

Go to the Workspace ONE Access console to configure adaptive management app policies to control device management levels for iOS devices enrolled without management. See [Managing Access Policies in the Workspace ONE Access Managing User Authentication Methods guide](#) on the page [VMware Workspace ONE Access documentation](#) page.

Configure Contact Email and Phone Number Information for Workspace ONE Intelligent Hub Support Tab

You can configure email and phone number contact information in the Workspace ONE UEM console to be used for end-user support. This information displays in the Workspace ONE Intelligent Hub app Support tab.

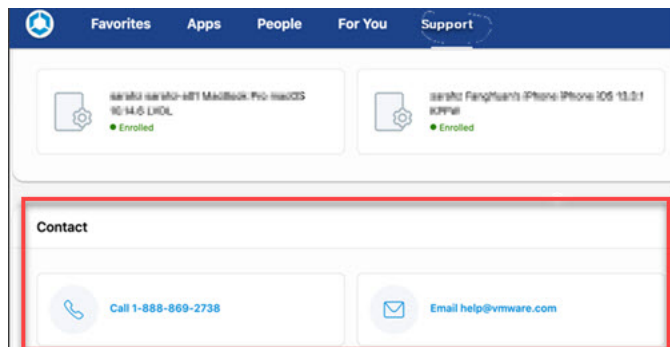
When you configure device enrollment settings in the Workspace ONE UEM console, the Customization tab includes two fields Enrollment Support Email and Enrollment Support Phone that displays example text. Replace the example text with your contact information.

Procedure

- 1 In the Workspace ONE UEM console, select your **Global > customer-level organization group** and navigate to the **Devices > Devices Settings > Devices & Users > General > Enrollment** page.
- 2 In the **Customization** tab, **Current Settings** section, select **Override**.
- 3 In the **Enrollment Support Email** text box, enter the email address that users can use to contact your support team.
- 4 In the **Enrollment Support Phone** text box, enter the phone number that users can call to contact your support team.
- 5 Click **Save**.

Results

This information displays in the Support tab.



Workspace ONE UEM Device Management Options for Public and Internal Apps

You can configure to deploy public and internal applications based on the device management status. Any device can access applications that are configured as open access apps. Only devices that are granted permission through the Workspace ONE Intelligent Hub app can access applications that are configured for managed access.

The table outlines capabilities for both managed and unmanaged scenarios.

Access Type	Features	Description	Suggested Uses
Open Access (unmanaged)	<ul style="list-style-type: none"> ■ Self-service app catalog for Web, Horizon, and Citrix resources. ■ Launch web/virtual with single sign-on (SSO). ■ Touch ID / PIN application protection. ■ Device jailbreak detection. ■ Support for Workspace ONE Access conditional access, including authentication policies and blocking devices. ■ Native application access. ■ Internal App and SDK app distribution. 	<p>Users access resources on their device without granting admins permission to access their device.</p> <p>The applications with open access are available to devices no matter their managed status. Admins cannot systematically remove native applications when they are set to Open Access.</p>	<ul style="list-style-type: none"> ■ Provide application access to end-users immediately upon login, without elevated security permissions. ■ Recommend the use of an application without requiring that the application is installed. Users can install the application on their device when they want. ■ Applications do not contain sensitive corporate data and do not access protected corporate resources. ■ To distribute applications to auxiliary personnel without the Workspace ONE UEM MDM profile.
Managed Access	<ul style="list-style-type: none"> ■ Self-service app catalog for Web, Horizon, and Citrix resources. ■ Launch web/virtual with single sign-on (SSO). ■ Touch ID / PIN application protection. ■ Device jailbreak detection. ■ Support for Workspace ONE Access conditional access, including authentication policies and blocking devices. ■ Managed and direct installation of Native Apps. ■ Internal App and SDK app management. ■ Support for app configuration. ■ Per-app VPN ■ One-Touch SSO for SAML enabled native apps. ■ Device profiles. ■ Workspace ONE UEM compliance engine. 	<p>Users install a management profile on their device to grant admins permission to access their device.</p> <p>Applications with managed access are available to devices that Workspace ONE UEM manages.</p> <p>If Workspace ONE UEM does not manage the device, Workspace ONE prompts the user on the device to enroll with Workspace ONE UEM. If the device is enrolled, the user can use the device to access the application through Workspace ONE.</p>	<ul style="list-style-type: none"> ■ To remove sensitive corporate data from devices when users leave the organization or lose their device. ■ Require app tunneling to authenticate and securely communicate with internal back-end resources when applications access the intranet. ■ Enable single sign-on for applications. ■ Track user adoption and installation status for applications. ■ Deploy the application automatically upon enrollment.

For information on where to configure managed access options for internal applications or how to add public application for deployment through Workspace ONE Intelligent Hub, see the Workspace ONE UEM Mobile Application Management Guide.

Managing Access to Applications in Workspace ONE UEM

A single user might be entitled to a mix of open or managed access to native apps. The adaptive management approach allows for end users to use open access applications without requiring management. When users request a native app that requires management, adaptive management provides the additional security and control needed to manage that native app.

When applications are managed, users must enable Hub Services to install and use the managed applications. When you upload an application in the Workspace ONE UEM console, the access state displays as either open or managed based on configuration for that application. For example, if the **Send App Configuration** option is selected, an application is set to require management.

Applications that require management display a star icon when viewed in an unmanaged state in the catalog. **Users must select to enable Workspace ONE services through the adaptive management process to use the application.** When users attempt to download an application that displays a star icon, they are prompted with a message that asks users to enroll. Users can click a privacy notice link to see the privacy impact for their personal information if they choose to continue with the adaptive management process. The privacy notice automatically pulls settings from the Workspace ONE UEM environment they are about to enroll into. After reviewing the privacy setting information, users can either proceed to enable MDM or back out and continue to use the Workspace ONE Intelligent Hub app unmanaged on their device. When users device is under MDM, the star icon is removed from all the managed applications.

Configuring Mobile Single Sign-On from Workspace ONE UEM Enrolled Devices

Configure mobile single sign-on (SSO) to allow users from Workspace ONE UEM enrolled devices to log in to their enabled applications securely without entering multiple passwords.

The devices that can be configured for SSO are iOS and Android devices.

iOS Single Sign-On Component Configuration

Mobile single sign-on for iOS uses the PKINIT Kerberos protocol for certificate transport, but does not require an on premises infrastructure. A built-in Kerberos adapter is available in the service, which can handle iOS authentication without the need for device communication to your internal domain controller. In addition, Workspace ONE UEM can distribute identity certificates to devices, eliminating the requirement to maintain an on-premises CA.

Supported Devices

- iOS Version 9 and later

Android Single Sign-On Component Configuration

Mobile single sign-on (SSO) for Android is an implementation of the certificate authentication method for Android devices managed in Workspace ONE UEM services. With mobile SSO, users can sign in to their device and securely access their Workspace ONE Intelligent Hub apps without reentering a password.

The VMware Tunnel mobile app is installed on the Android device to add certificate and device ID information into authentication flows. The Tunnel settings are configured in the Workspace ONE UEM console to access the Workspace ONE Access service for authentication, and the service retrieves the certificate from the device for authentication.

Supported Devices

- Android 4.4 and later
- Applications must support SAML or another supported federation standard.

Deploying the Workspace ONE Intelligent Hub app to all Android devices does not automatically deploy the application Android for Work containers. Android for Work is required to use the Adaptive Management feature. To add this application to Android for Work devices as well and for more detail on the additional options available as part of Workspace ONE UEM MAM, review the Workspace ONE UEM Integration with Android for Work guide.

Set Up Workspace ONE UEM Enterprise Mobility Management on Google for Android

To manage Android devices in Workspace ONE, you must register Workspace ONE UEM as the Enterprise Mobility Management (EMM) provider with Google. The wizard walks you through the steps to register Workspace ONE UEM as the EMM provider.

Note If you are deploying the G Suite, see the VMware Workspace ONE UEM Integration with Android for Work guide on the [Workspace ONE UEM documentation landing page](#) for configuration details.

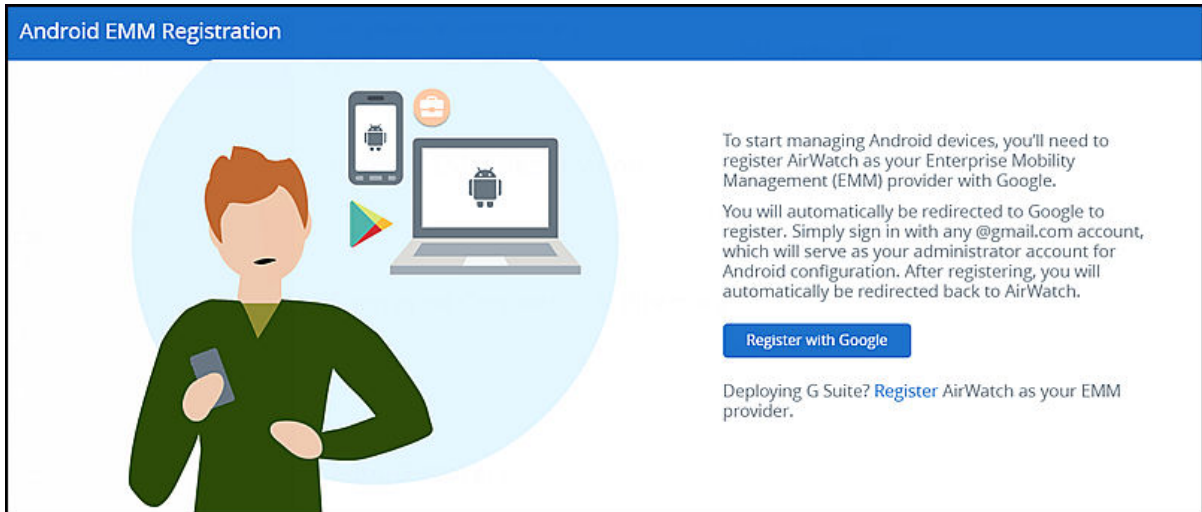
Prerequisites

A Google user account.

Procedure

- 1 Select the organization group for Workspace ONE Intelligent Hub from the Global list.
- 2 Click **Getting Started** in the left navigation pane.
- 3 In the Getting Started > Workspace ONE Intelligent Hub section, click **Start Wizard**.

- In the Android EMM Registration section, click **Configure**.



- Click **Register with Google**.

You are redirected to Google Play to add your organization name. The EMM provider is already populated with Workspace ONE UEM.

- Complete the configuration on the page and click **CONFIRM**.

- Click **COMPLETE REGISTRATION**.

You are returned to the Workspace ONE UEM console, Android for Work page. The Google Admin Console and API settings have been added to the page.

- Click **Save** and then **Test Connection**.

Results

You are now ready to enroll Android devices using Android Enterprise.

Deep Links to Workspace ONE Intelligent Hub Pages Supported on iOS and Android Devices

13

You can add a deep link in your notifications that takes the recipient of the notification directly to the specific page in the Workspace ONE Intelligent Hub app from their iOS devices.

The following deep links are supported for the Workspace ONE Intelligent Hub app on iOS and Android devices.

Deep Link URL to Favorites Tab

Deep link URL for iOS devices	Deep link URL for Android devices
wsonehub://favorites	
wsonehub://weblinks/new	

Deep Link URL to Apps Tab

Deep link URL for iOS devices	Deep link URL for Android devices
wsonehub://apps	wsonehub://apps
wsonehub://apps/view	wsonehub://apps/view
wsonehub://apps/view?name=browser	wsonehub://apps/view?name=browser
wsonehub://apps/view?name=Workspace%20one%20notebook	wsonehub://apps/view?name=Workspace%20one%20notebook
wsonehub://apps/view/browser	wsonehub://apps/view/browser
wsonehub://apps/view?ios=com.air-watch.boxer	
wsonehub://apps/view?ios=com.vmware	wsonehub://apps/view?android=com.vmware
wsonehub://apps/view/com.air-watch.boxer	wsonehub://apps/view/com.air-watch.boxer
	wsonehub://apps/view?android=com.boxer.email

Deep Link URL to People Tab

Deep link URL for iOS devices	Deep link URL for Android devices
wsonehub://people	wsonehub://people
wsonehub://people/view	wsonehub://people/view

Deep Link URL to For You Notification Tab

Deep link URL for iOS device	Deep link URL for Android device
wsonehub://foryou	
wsonehub://foryou/view	

Deep Link URL to Home Tab

Deep link URL for iOS device	Deep link URL for Android device
wsonehub://home	wsonehub://home

Deep Link URL to Support Tab

Deep link URL for iOS device	Deep link URL for Android device
wsonehub://support	
wsonehub://support/view	

Deploying Workspace ONE Intelligent Hub App

14

The Workspace ONE Intelligent Hub app can be installed on iOS, Android, macOS, and WindowsOS devices to manage devices and access resources. In addition, a web browser experience with Hub Services is available with Workspace ONE Access with or without incorporating Workspace ONE UEM.

The Workspace ONE Intelligent Hub interface offers a similar experience and options on any smart phone, tablet, or desktop computer.

Read the following topics next:

- [Distributing the Workspace ONE Intelligent Hub Application for iOS and Android](#)
- [Workspace ONE UEM Application Configuration for Enterprise Key Value Pairs](#)
- [Deploying Workspace ONE Intelligent Hub App for macOS](#)
- [How to Access the Intelligent Hub Portal from Web Browsers](#)

Distributing the Workspace ONE Intelligent Hub Application for iOS and Android

Users can either download the VMware Workspace ONE Intelligent Hub app from their device app store or administrators can configure Workspace ONE UEM to push the Workspace ONE Intelligent Hub application as a managed application to devices.

You deploy the Workspace ONE Intelligent Hub app from the Workspace ONE UEM console to specific groups and users within your organization. After users sign into the Workspace ONE Intelligent Hub app on their devices, they can access Web and SaaS apps that are entitled to them.

The following steps are to push the Workspace ONE Intelligent Hub app as a managed application from the Workspace ONE UEM console.

Note For detailed information on configuring managed applications in Workspace ONE UEM, see the VMware Workspace ONE UEM Application Management guide, available in the [VMware Workspace ONE UEM](#) documentation center.

Prerequisites

If you are planning to push the Workspace ONE Intelligent Hub app from the Workspace ONE UEM console, prepare Smart Groups of end users who are entitled to the app.

Procedure

- 1 In the Workspace ONE UEM console, navigate to **Apps & Books > Applications > Native > Public**, and select **Add Application**.
- 2 Select the platform, either **iOS** or **Android**.
- 3 Select **Search App Store**, and in the **Name** text box enter **Workspace ONE** as the key word to find the **Intelligent Hub** app in the App Store.
- 4 Choose **Next**, and use **Select** to upload the Workspace ONE Intelligent Hub application from the App Store Result page.
- 5 Configure the assignment and deployment options for Workspace ONE Intelligent Hub users in the following tab settings.

Tab	Description
Info	Enter and view information concerning supported device models, ratings, and categories.
Assignment	Assign the Workspace ONE Intelligent Hub apps to smart groups of end users who can use the application on their device.
Deployment	Configure availability and advanced enterprise mobility management (EMM) features, if applicable. To automatically configure managed applications, enable Send Application Configuration and enter the App Configuration for Enterprise (ACE) key value pairs. See Workspace ONE UEM Application Configuration for Enterprise Key Value Pairs .
Terms of Use	(Optional) Enable Terms of Use for using the Workspace ONE Intelligent Hub application.

- 6 Select **Save & Publish** to make the application available to users.
Complete these steps for each supported platform.

Workspace ONE UEM Application Configuration for Enterprise Key Value Pairs

When deploying the Workspace ONE Intelligent Hub app as a managed application in Workspace ONE UEM and you enable Send Application Configurations when you push the app from the Workspace ONE UEM console, you can preconfigure Workspace ONE Intelligent Hub settings that are applied when users install and start the Workspace ONE Intelligent Hub app.

When the app is uploaded to the Workspace ONE UEM console as a managed mobile application, you can configure the VMware Workspace ONE UEM URL, the device UID value, and requirement for certificate authentication in Android devices.

Table 14-1. Intelligent Hub Managed Device Configurations Options in Workspace ONE UEM Console

Platform	Configuration Key	Value Type	Configuration Value	Explanation
All	AppServiceHost	String	<VMware Workspace ONE UEM Server URL>	Configures the server URL for VMware Workspace ONE Intelligent Hub on devices.
iOS	deviceUDID	String	{DeviceUid} Enter the device UID value. Do not use the Insert Lookup Value function.	Tracks the devices used to authenticate to the Workspace ONE Access environment.
iOS	SkipDiscoveryScreen	Boolean	true	When set to True, Intelligent Hub tries to move past the email address/server URL screen. When used with the AppServiceHost configuration key, users are immediately taken to the authentication screen. If mobile SSO is also used, admins can provide end users with a seamless experience whereby they start Intelligent Hub and immediately begin loading their Intelligent Hub app.

Table 14-1. Intelligent Hub Managed Device Configurations Options in Workspace ONE UEM Console (continued)

Platform	Configuration Key	Value Type	Configuration Value	Explanation
Android and iOS	RemoveAccountSignOut	Integer	0 - The Remove Account option displays 1 - The Remove Account option does not display If the value is not set, the Remove Account option is displayed.	When the value is set to 1, the Remove Account option does not display in the users app Settings page. Users cannot remove the Intelligent Hub account from their device. When this value is set to 0 or no value is set, the Remove Account option displays. If users click Remove Account, Workspace ONE UEM performs an enterprise wipe of the device and unenrolls the device from Workspace ONE UEM.

rev

Deploying Workspace ONE Intelligent Hub App for macOS

The Workspace ONE Intelligent Hub-based enrollment process secures a connection between macOS devices and your Workspace ONE UEM environment. Install the Workspace ONE Intelligent Hub app to facilitate the enrollment and enable the real-time management and access to the relevant device information.

Two methods are available to introduce users to the Workspace ONE Intelligent Hub app.

You can configure settings to automatically install the Workspace ONE Intelligent Hub app to devices immediately after enrollment is finished.

- 1 In the Workspace ONE UEM console, go to **Settings > Device & Users > Apple > Apple macOS > Intelligent Hub Settings**.
- 2 To enable automatic deployment of the app to devices when users enroll through the Web or DEP, make sure that **Install Hub after Enrollment** is enabled.
- 3 Save your changes.

Users who do not have an enrolled device can also install the Workspace ONE Intelligent Hub app. The app prompts users to enroll their device before they can access corporate resources. Users can navigate to <https://getwsone.com> and download the Workspace ONE Intelligent Hub app installer to their devices.

See the macOS Device Management guide on the [Workspace ONE UEM](#) documentation landing page to install, configure, and manage macOS devices with Workspace ONE UEM.

How to Access the Intelligent Hub Portal from Web Browsers

Users can access the Intelligent Hub web portal in the latest versions of the following browsers, Mozilla Firefox, Google Chrome, Safari, and Microsoft Edge.

When you configure apps, you can specify that apps can be opened only in the VMware Browser app, if you want to restrict how users access their apps. See the VMware Browser documentation on the Workspace ONE UEM documentation site.

User Experience in the Workspace ONE Intelligent Hub App

15

The VMware Workspace ONE® Intelligent Hub app offers a single destination where users can securely access, discover, connect with, and act on their corporate resources, teams, and workflows.

The Workspace ONE Intelligent Hub app provides a simple, unified onboarding experience securing both corporate and personal devices. The app also lets organizations enable capabilities like a unified catalog to access business apps, actionable notifications to keep employees informed, people directory to break silos, and custom tab to allow easy access to corporate resources through Hub Services integration.

The Workspace ONE Intelligent Hub app can be installed on iOS, Android, macOS, and Windows devices to manage access to company resources.

The Workspace ONE Intelligent Hub user interface works similarly on phones, tablets, and desktops. The catalog page displays the apps that are added as resources for the user. Users can tap or click to search, add, mark apps as favorites, and update their list of available apps and users can receive notifications and act upon them directly from the app.

Read the following topics next:

- [Installing and Setting Up Workspace ONE Intelligent Hub App on Devices](#)
- [Setting Passcodes Before Accessing the Workspace ONE Intelligent Hub App](#)
- [User Experience When Accessing Apps from the Workspace ONE Intelligent Hub App](#)
- [Workspace ONE Intelligent Hub App Account Settings](#)
- [Using People Functionality in the Workspace ONE Intelligent Hub App](#)
- [Receiving Notifications in the Workspace ONE Intelligent Hub App](#)
- [Accessing Native Apps in Workspace ONE Intelligent Hub](#)
- [User Experience When Accessing Workspace ONE Intelligent Hub Portal in a Web Browser](#)
- [Account Settings Available in the Workspace ONE Intelligent Hub Web Browser View](#)

Installing and Setting Up Workspace ONE Intelligent Hub App on Devices

Users can either download the Workspace ONE Intelligent Hub app from their device app store or administrators can configure Workspace ONE UEM to push the Intelligent Hub app as a managed application to devices.

When users initially install the app, they navigate through a series of screens to prepare them for setting up their device in management mode and install and enable their Workspace Services profile that is used to separate work and personal data on their device.

Privacy and Data Sharing

VMware Workspace ONE Intelligent Hub app collects information to provide secure access to users work data and apps. Users see a privacy and data sharing notice that they must accept. The privacy notice displays the following information.

- Data collected by Hub – Provides a summary of data that is collected and processed by the application. Some of this data is visible to the administrators of the Workspace ONE UEM administration console.
- Hub Permissions – Provides a summary of device permissions requested for the app to enable product features and functionality, such as push notifications to the device. These permissions can be changed at any time within the user's device settings but change might impact the app functionality.
- Company's Privacy Policy – By default, a message is displayed for users to get more information about your company. When configured by the administrator, tap Your Company's Privacy Policy to access the employer's privacy policy information.

Setting Passcodes Before Accessing the Workspace ONE Intelligent Hub App

Users must have the locked passcode feature enabled on their devices. If this option is not enabled, the first time the Workspace ONE Intelligent Hub app is launched, users are asked to create a passcode. This passcode is entered whenever users access the Intelligent Hub from their device.

Where the passcode is set on a device depends on the platform. For Android devices, the passcode is set at the app level. For Window desktop devices and for iOS devices, the passcode is set at the device level.

Note iOS and Android devices also support the Touch ID fingerprint sensing functionality.

The Workspace ONE Intelligent Hub app can detect possible security issues on devices. If users deactivate the passcode on the device, the next time they access the Workspace ONE Intelligent Hub app, they are prompted to set a passcode. When an app-level passcode is enabled, users cannot deactivate their app level passcode.

User Experience When Accessing Apps from the Workspace ONE Intelligent Hub App

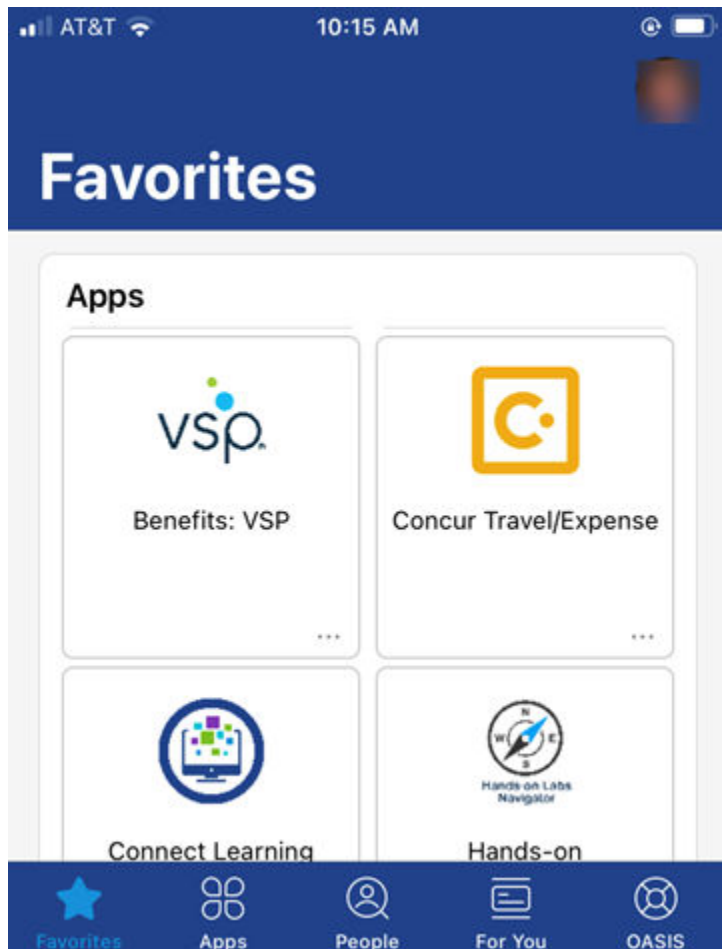
Users can access their apps, and install web, mobile, and virtual applications that they are entitled to. Web and virtual apps can be opened directly from the user's portal. Native apps, such as iOS and Android apps, are launched from the device springboard.

The catalog page layout that you configured in Hub Services displays when users open the Workspace ONE Intelligent Hub app on devices or in Hub portal view.

In the Workspace ONE Intelligent Hub app view, any apps or categories you selected to promote are displayed at the top of the Apps pane view. New apps display in the new apps section. When apps are organized into logical categories, these categories are displayed. People, Notification, and Support tabs are in the navigation pane.

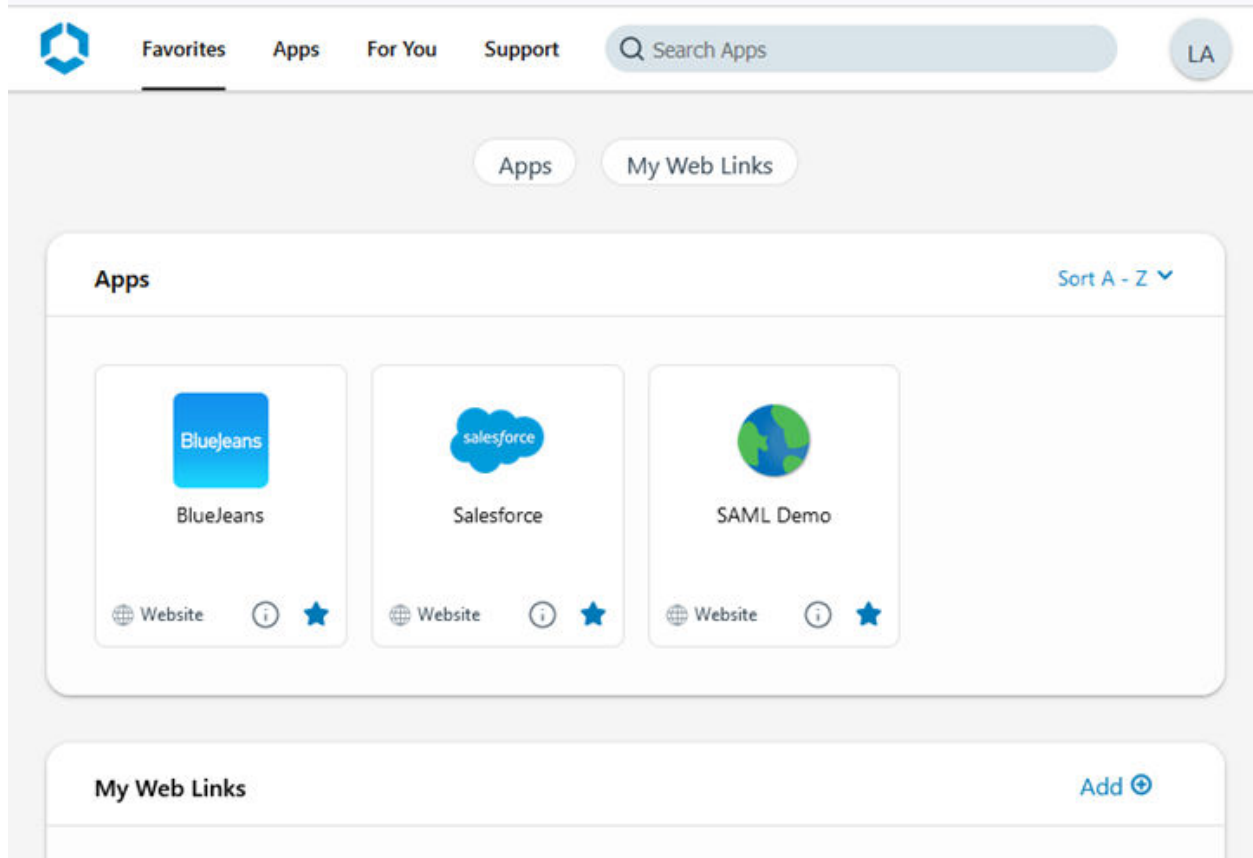
Note Apps and desktops from Horizon Cloud Service on Microsoft Azure with Universal Broker is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

Figure 15-1. Workspace ONE Intelligent Hub on a Device



In the Workspace ONE Intelligent Hub view from a browser, The navigation tabs are at top of the page along with the search bar to search for app. If you enabled Favorites, the Favorites tab displays before the Apps tab.

Figure 15-2. Workspace ONE Intelligent Hub Web Portal View



Workspace ONE Intelligent Hub App Account Settings

Users click their photo icon in the top right corner of the screen on their device to access the Workspace ONE Intelligent Hub account settings.

- **Notifications.** Users enable or deactivate push notifications that are sent from the Workspace ONE Intelligent Hub app.
- **Legal and Privacy** information can be viewed.
- **About.** In About users can view the Workspace ONE Intelligent Hub app version that is installed.

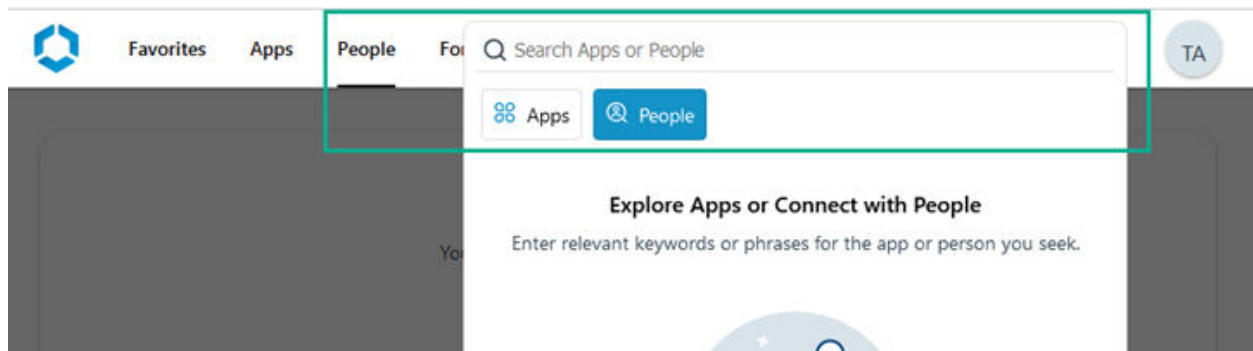
- **Change Password.** When Change Password is displayed, users can change their Active Directory password from the Workspace ONE Intelligent Hub app whenever they want.

Note This feature is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

Using People Functionality in the Workspace ONE Intelligent Hub App

When the People feature is enabled in Hub Services, employees can search their organization's active directory from the Workspace ONE Intelligent Hub app to view colleague details and organization charts.

When employees click the People tab, they might see their reporting hierarchy. They can click the search icon to type names of people in their organization to find contact information.



When they select a contact from the search results, they can view the colleague's profile, which can include email addresses, phone number, and office addresses. They can click the organization link to see the hierarchy and navigate to other colleagues in the organization.

Employees can click links on the profile page to send a quick email or call their colleague.

Note This feature is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

Receiving Notifications in the Workspace ONE Intelligent Hub App

When you enable the notifications feature in Hub Services, employees can receive actionable, real-time messages, including push notifications in the Workspace ONE Intelligent Hub For You tab on their devices and from the Hub portal.

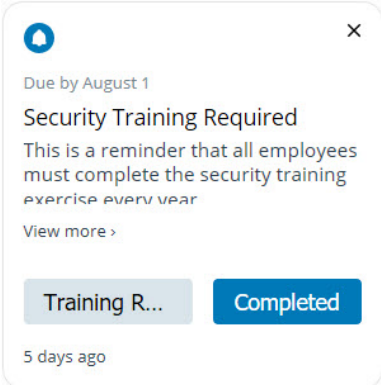

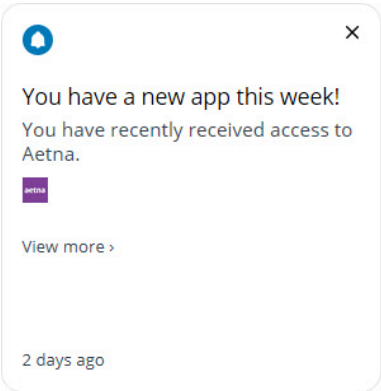
A notification count is displayed on the For You tab if there are unread or priority notifications. If no notifications are listed, when users click For You, the message reads **You are all caught up!**

Most messages are sent as standard notifications. You can prioritize notifications as either high-priority or urgent for information that is critical for the user to review and respond to on a timely basis. High-priority messages are displayed at the top of the For You page in the Priority section above Actionable and Informational notifications.

Users might also see a banner informing them of the incoming priority notification. They can click the banner to go to the For You page. The notification count in the For You bell icon counts high-priority notifications until the user takes actions on the notification request. See [Creating Custom Notifications in Workspace ONE Hub Services](#)

Urgent messages display on top of the app page until the users takes an action on the notification. Users cannot proceed to another screen until all urgent notifications are acted on.

Table 15-1. Types of Notifications Received in Workspace ONE Intelligent Hub App

<p>Custom Notifications</p>	<p>As an admin, you can create custom notifications.</p> 
<p>Approval Request</p>	<p>Users can approve or deny approval notifications.</p> 
<p>New App Availability</p>	<p>If New Apps Notification is enabled, users receive a weekly notification about new apps that are available. They can click the link in the notification to learn more about the app and to add the app to their catalog.</p> 

When users click an action button to respond to the notification, the notification is moved to the History folder. The notification is archived in the History folder for 90 days, after which it is deleted.

The setting to receive notifications is enabled in the Workspace ONE Intelligent Hub app. Users can manage the Notification setting in the Workspace ONE Intelligent Hub app user's Account page.

How users manage notifications on their devices

The setting to receive notifications on mobile devices is enabled by default in the Workspace ONE Intelligent Hub app. Users can deactivate the notification setting from the Account page accessed from their profile photo icon in the app.

Accessing Native Apps in Workspace ONE Intelligent Hub

Native apps are application programs that are developed for a specific mobile device. Users can see their Workspace ONE UEM-entitled native apps from the Workspace ONE Intelligent Hub catalog page. For example, if a user is viewing the catalog from an iOS device, only iOS applications entitled to the user are shown.

In the catalog page, users tap Install to install the app on their device. Upon tapping Install, a pop-up window appears to inform users of what is happening next. The information displayed is based on the app type and platform.

Native apps can be marked as favorite and are displayed in the Favorite section in the Workspace ONE Intelligent Hub app.

If an app requires that the iOS device be managed by Workspace ONE UEM, when an end user attempts to download that app, a Require Management message displays.

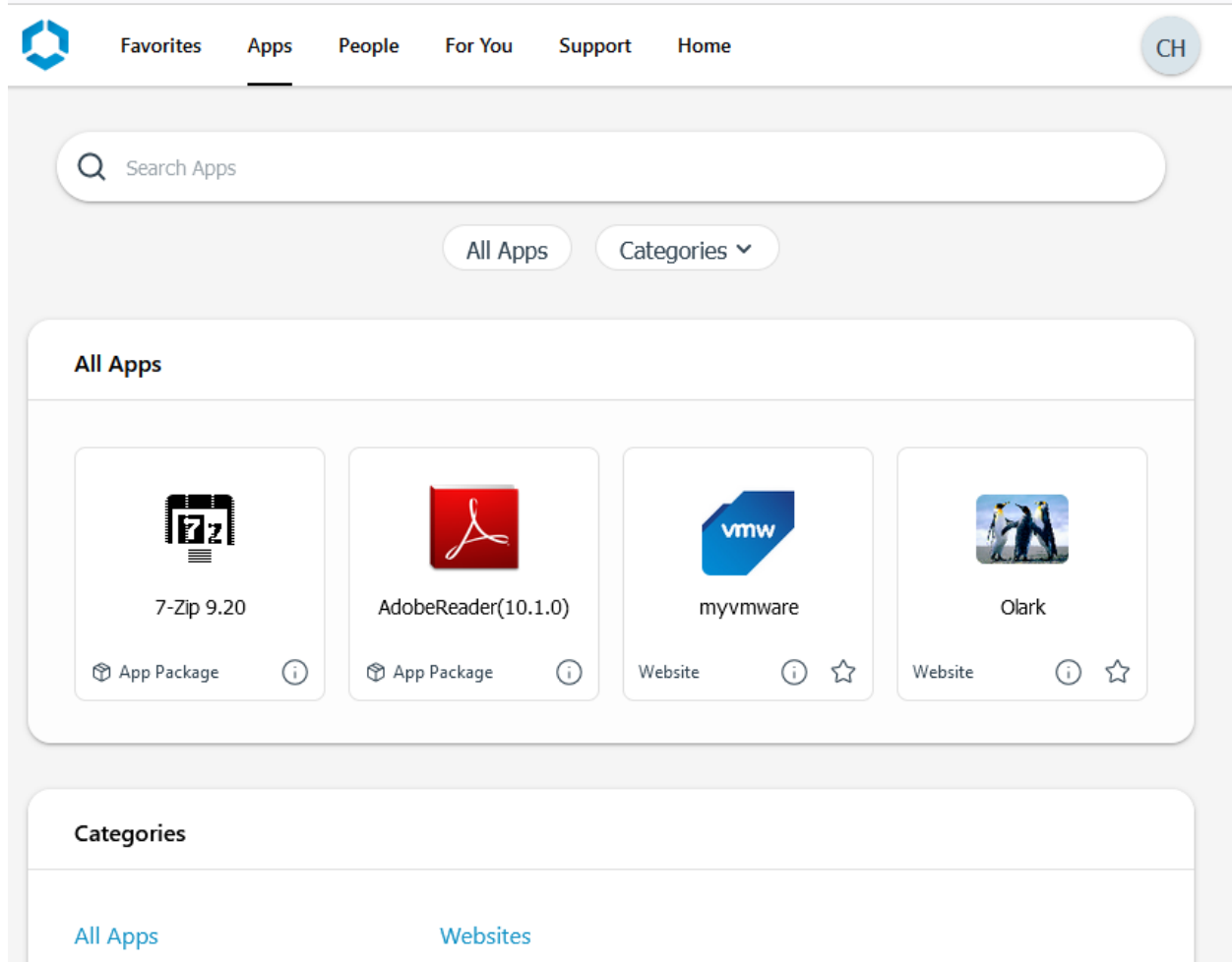
User Experience When Accessing Workspace ONE Intelligent Hub Portal in a Web Browser

When users go to the Workspace ONE Intelligent Hub portal, the browser displays the feature tabs that you enabled in Hub Services.

Users can access apps that are assigned to them, mark them as favorites, search for people in the organization, receive notifications in the For You tab, get help from a support tab, and go to the custom tab link that you set up.

Note Mobile applications are not available from the Hub portal view in a browser.

Figure 15-3. Workspace ONE Intelligent Hub Portal View in Web Browser



Account Settings Available in the Workspace ONE Intelligent Hub Web Browser View

When users are in the Workspace ONE Intelligent Hub web portal, they can click their name in the upper-right corner to see the account settings and to sign out.

If you configured the **Change Password** option, users can click **Change Password** to change their password.

Note This feature is not available for a Workspace ONE Access tenant that has VMware Identity Services enabled. See the *Unsupported Workspace ONE Features* topic in the [Configuring User Provisioning and Identity Federation with VMware Identity Services](#) guide.

In the account preferences section, the following settings are available.

- Appearance.** Users can select to display Workspace ONE Intelligent Hub app screens in dark mode.

- **Horizon Remote Apps.** Users can select how their Horizon remote apps open on their devices, either in the Horizon Client or in a browser. They cannot set a default launch preference in the Workspace ONE Intelligent Hub app.

Frequently Asked Questions about the VMware Workspace ONE Intelligent Hub App

16

This FAQ answers frequently asked questions about how to use the features in the Workspace ONE Intelligent Hub application.

A number of these features require customization by your IT administrator so your specific use cases might differ from what is described in these FAQ answers. Some features might not be available for all users. If you have questions or want some of these features enabled, reach out to your IT administrator.

Note How to contact your IT administrator can often be found in the Support tab in Workspace ONE Intelligent Hub.

I'm new. Start Here.

What is Workspace ONE Intelligent Hub?

The Workspace ONE Intelligent Hub app can be installed on iOS, Android, macOS, and Windows devices and allows you to access, discover, and connect with corporate resources, teams, and workflows within your company. Using this app enables you to be productive while staying compliant with your company's security policies.

If your company enabled access from the Hub web browser, you can access your web applications, notifications, and support information from the Hub portal in a browser.

Why do I need Workspace ONE Intelligent Hub?

You need the Workspace ONE Intelligent Hub app to be able to add work resources on your devices. The device can be your laptop or desktop as well as your mobile device. Your company is using Workspace ONE Intelligent Hub to configure, secure and deploy their work tools onto your device to improve your employee experience.

The Workspace ONE Intelligent Hub app can provide access to the following types of services.

- **Favorites** – Bookmark apps and other services you use frequently and want to easily access.
- **Apps** – Provides you with a unified catalog of available native, web, and virtual applications that your company deployed as your work tools.
- **For You** – Provides a notification center where you can receive company administered push and in-app notifications.

- **People** – Provides you with quick access to colleague's information through an employee directory. You can also see the colleague's organization chart with name, email, phone.
- **Self-Service Support** – Provides helpful links to help you perform basic device management tasks when you need help with any of your devices. You can find information about who to contact if you have problems with your enrolled device.
- **Home** – Gives you access to your company resources by linking to an intranet or company portal.

What about my privacy?

Privacy is a fundamental right and VMware believes that you should have complete control and visibility into the information you share.

If your company has given you the choice to use one device for work and personal use, there may be information you want to keep personal. Workspace ONE works to provide complete transparency into what data is being collected, through a privacy notice built into each of our apps. The privacy notice is presented when you are first getting started in the app. Anytime a change is made that could impact your privacy you will be alerted, and you can review the privacy notice at any time.

Your IT department selected Workspace ONE because it protects them and you. Your company's priority is to secure the corporate apps and data on your device, while only capturing the minimal amount of information needed to do that.

Make sure to read VMware's Privacy Policy for the most up to date information: <https://www.vmware.com/help/privacy.html>

Can Workspace ONE Intelligent Hub see my browsing history?

The Workspace ONE Intelligent Hub application does not monitor your personal browsing traffic. If you are using company resources (including device management) there is a chance that your company might have other systems that monitor traffic into and out of their network. Some of these applications that are on your device (e.g. utilizing proxies, Tunnel SDK or VPN) transfer data through your company's network.

What if I delete Workspace ONE Intelligent Hub?

Depending on your company's configuration of the Workspace ONE Intelligent Hub app, merely deleting the app could have a negative impact on the behavior of the device and applications.

If the intent is to remove work resources from your device, unenroll the device from Workspace ONE UEM device management. You might be able to do so through the Workspace ONE Intelligent Hub app or by reaching out to your IT admin.

If you deleted the app from your device without unenrolling from Workspace ONE UEM, you might be able to download it again and log back in to access your work resources again.

How do I log into Workspace ONE Intelligent Hub?

Before you can log in to Workspace ONE Intelligent Hub, your administrator must create an account for you in their system and let you know what credentials are required to access the app. The login credentials that you use for Workspace ONE Intelligent Hub might be the same used to access other company systems but could also be unique.

Some companies allow all employees access to the work resources on all their devices. Companies can also require that you request access to resources for multiple devices.

If you use a computer that is configured with Workspace ONE, logging into the computer for the first time can include configuring Workspace ONE Intelligent Hub and downloading all your work applications and configuring access without having to visit IT.

Apps are being added and deleted automatically from my device. What's going on?

When you use the Workspace ONE Intelligent Hub app to enroll your device into Workspace ONE UEM, applications and configuration profiles can be deployed to your device where they automatically install in the background. When applications are deemed unnecessary or you have unenrolled your device, apps can disappear from your device.

I don't see my question here, what can I do?

First off, thank you for your inquiry to help improve our products.

Reach out to your IT administrator and they can escalate questions to us. We want you to talk to your IT admin because there are several ways that your company can configure our software to fit their needs. If they determine that your question is not something they are able to resolve, they can reach out to our teams to collaborate on a solution.

Enrollment and Login

My company gave me a QR code to use, how does that help me?

This QR code, if generated by our system, allows you to scan the code with the Workspace ONE Intelligent Hub app for Android or iOS devices to prefill in most information or even log you into your account to begin the configuration process on your device.

How do I enroll (first time login and setup) into Workspace ONE Intelligent Hub?

There are several ways to enroll into Workspace ONE Intelligent Hub. Following are the most common ones.

1 Email Address

This method allows you to simply enter your corporate email and behind the scenes, the Workspace ONE Intelligent Hub app finds the correct environment details for your company and allows you to complete the authentication.

2 Server Name

You provide the specific server name/URL that your company provisioned and possibly a Group ID, which narrows down the exact location where you are registering.

3 QR Code / Deep Link

A streamlined way which pre-fills the information such as the server URL and Group ID without having you type it.

What can I do when I get the "Device Not Approved" message?

Your organization can evaluate the type of devices to approve. They can regulate the number of devices, the type of device (platform, model, manufacturer), the minimum operating system version, or other restrictions to determine which devices are allowed to enroll.

Contact your admin to find out what devices are supported. In general, recent devices with the most up to date operating systems are supported.

How can I unenroll or completely remove work data from my device?

Depending on how your organization is configured, you might be able to unenroll yourself.

To unenroll

- 1 Launch Workspace ONE Intelligent Hub.
- 2 Navigate to the Support Tab or the Account section via the icon at the top right hand corner.
- 3 Select your current device.
- 4 Select "Enrollment".
- 5 Tap "Unenroll Device".

This process can take a few seconds to a couple of minutes to remove all the corporate information from the device.

If you are on a Bring Your Own Device (BYOD) setup and your IT admin has configured this, only your work information is deleted. All of your personal information stays on the device.

If I unenroll, will it affect any of my personal data on my device?

This depends on your organization's configuration. If your IT admin configured the device for Bring Your Own Device (BYOD) then your personal data remains on the device after you unenroll your device. If your IT admin configured the company owned device to wipe completely, any personal data on that device will be lost.

What is a Check In/Check Out system?

Check In/Check Out is a system that is generally used when there are multiple users of a single device. Think of the situation where someone clocks in, checks out a device, performs their job and once the job is complete, they check the device back in and clock out.

This means that anyone set up for Check In/Check Out can pick up any device configured with Check In/Check Out, log in and do their job. If that device breaks or the battery runs out, they can check out another device and log in as easily as they did to the first one and get access to all their same work tools.

Why do I need a password/passcode?

Passwords or passcodes can be required to unlock your device and can also be required to open Workspace ONE Intelligent Hub apps that are on your device.

In either case, if your organization enabled this as a security requirement, you set a passcode for your device (which enables device level encryption) and also set an app-level passcodes to secure the Workspace ONE Intelligent Hub app.

What credentials do I use?

This really depends on your organization's configuration.

Typically, it will be your Active Directory credentials or a specific username/password for the Workspace ONE system.

Other options might be a single-use token, MFA/2FA, or a certificate.

If you are uncertain, check with you IT administrator.

What is the difference between Corporate owned and Employee owned?

Corporate owned devices are devices that are owned by your company. Corporate owned devices are often fully managed and controlled either from the manufacturer or with our software. It is not recommended to store any personal information on these types of devices because companies can completely factory reset these devices.

Employee owned or Bring Your Own Device (BYOD) use cases are where you bring your personal device and are able to enroll your device to add your work resources on your device. All your personal information and data is kept separate from the company's data. Companies can remove corporate data from your device but are unable to remove your personal data.

There are other enrollment methods that are not as common such as Corporate Owned Personally Enrolled (COPE) where a company has full ownership over the device, but the intent is for one person to use that device for work as well as anything personal that they want to.

See our other FAQs on Privacy to learn about what information your company can and cannot see.

What is the difference between Device Managed, User Managed, and Registered?

Managed/Fully Manager/Device Managed is device management where VMware Workspace ONE leverages the platform APIs to manage the device.

Registered Mode is where a registration is created in Workspace ONE UEM via an "anchor application" like Workspace ONE Intelligent Hub to facilitate a lighter level of management.

Adaptive Management is a term used for when a device is moved from "Registered Mode"/"MAM" to mobile device management (MDM), when end users request to select an app that requires management

Step-Up Enrollment is a comparable term used for Adaptive Management. This represents the process of stepping up from Registered Mode to MDM.

MAM-Only (Mobile Application Management), Unmanaged, Container, Standalone Boxer:

Terms used to represent a non-MDM mode of enrollment/management

User Enrollment is an Apple specific enrollment implementation designed for BYOD where the user, not the company, owns the device.

Work Profile can be set up on an Android device to separate work apps and data from personal apps and data. With a work profile, you can securely and privately use the same device for work and personal purposes—your company manages your work apps and data while your personal apps, data, and usage remain private.

Why do I have to reauthenticate?

Your authentication credentials are configured to expire for various reasons. When the access token expires, you will be asked to reauthenticate. Examples of when you must reauthenticate.

- An app that requires a password to access is configured to require reauthentication after a configured specified time of in activity.
- You have not accessed your Workspace ONE Intelligent Hub app in a while and the refresh token has expired. In this case, you could be prompted to reauthenticate with Workspace ONE Access or your company's Identity Provider (Ping, Okta, Azure AD). Typically refresh token are set to expire after 7 to 10 days of inactivity.
- If you use Hash-based message authentication (HMAC), the HMAC token might be lost or has been invalidated. Workspace ONE Intelligent Hub requires you to reestablish your identity with the Workspace ONE UEM system.

What can I do if I get a message that says, "Invalid User Credentials"?

If you are seeing this message during the enrollment flow, the provided credentials do not match the expected input. This could be a situation where there's a different username/password/token combination.

For specific on how to address this sort of situation, contact your IT administrator.

Apps/Catalog/Favorites Tab

What is the App Catalog?

The Apps tab or the App catalog is a unified location for native, web, and virtual applications assigned to your user account.

Public native applications that can be downloaded from the App Store or Google Play Store, and white-label internal native applications that your company developed can be downloaded and installed from the Catalog.

Your company might also curate web apps (websites, web clips, or SaaS apps) for use in your job. Additionally, you might have virtual apps/desktops available to launch and use.

The App catalog allows you to install, launch, update as well as reinstall applications.

Hint: press the thumbs up icon to let others in the company know that you like a certain app! And you can press the star icon to add it to your Favorites Tab for easier access!

What types of apps can I have?

The Apps tab (App catalog) gathers together multiple types of apps and resources and will show or hide some based on the device you are on. Types of apps included in the App catalog.

- Native Applications. These apps display on the platform that supports them.
 - Public - available in the platform's application store (ex. App Store, Google Play Store).
 - Internal applications. - These apps are developed and deployed either by your company or specific for your company by a third party.
- Web Applications
 - Websites
 - Web clips
 - SaaS apps
- Virtual Applications
 - Horizon
 - Citrix
- Saved Bookmarks - these are websites that you can add and bookmark for easy access via the Workspace ONE Intelligent Hub application on any supported platform.

How do I get/install/update my apps?

Apps that are natively built for your device can be installed from the Apps tab if you see an **Install** next to an app.

When you press **Install**, it will send a command to the server to push that application down to the device.

If you manually install apps from the App Store, there is a chance that you will have to approve management of that application so your company is able to securely deliver work resources.

When you see an "Update" option, a newer/later version of the application is available. Pressing "Update" will trigger an installation of the latest available version.

What is the Favorites Tab?

The Favorites tab is a tab that will show all the apps and websites that you starred in Workspace ONE Intelligent Hub. These favorites sync across all your devices so if you starred an item on the Hub web portal, that item will also show up starred on your mobile and computer versions of Workspace ONE Intelligent Hub. The starring feature can be found in the overflow menu of an app's icon or in the details page of that specific app.

Users are also able to save their own bookmarks that will show up in the Favorites tab on all devices.

The Favorites tab can be configured by your administrator therefore depending on configuration, features mentioned above might not be available for all users.

Will my Favorited (Starred) items also show up on my other devices?

Yes! Starred items and your bookmarks will show up across different devices if they are supported on that platform

Additional Hub Tabs/Features

What is the People Tab?

The People tab connects to your company's internal directory so you can search for and learn about colleagues, quickly contact them or see their team structure.

This tab requires configuration by your administrator therefore features mentioned above might not be available for all users.

What is the Home/Custom Tab? (Can be renamed by your company)

This is a tab that your admin can set to be a specific website that they determined is important for you. This could be an internal main company website or site that links to other essential resources. The name of the tab can be changed by your admin but presents as a full web page .

This tab requires configuration by your administrator therefore features mentioned above might not be available for all users.

What is the For You Tab?

For You is the tab where notifications your company has sent you are displayed. This can include notifications about new apps that you have access to or rich notifications that persist for a certain amount of time or include additional assets like surveys, images, videos, links, and other attachments.

Additional features of notifications in the For You tab include the ability to approve requests that come from other systems such as expense reporting, deal adjustments or other company specific use cases.

This tab requires configuration by your administrator therefore features mentioned above might not be available for all users.

What is the Support Tab? (Can be renamed by your company)

The Support tab is your go-to place when you need help with any of your devices. Your admin can configure helpful links that display in this tab. You can see and manage your devices such as installing or reinstalling profiles and can include support contact information in the case you are unable to remedy your issue.

This tab requires configuration by your administrator therefore features mentioned above might not be available for all users.

[iOS] What is a Profile and why do I need to install it?

Profiles are sometimes required by your company to configure your device for things like email accounts, device passcode options and other functions like allowing you to connect to protected Wi-Fi networks without knowing the password or automatically configuring your VPN to access your company's internal network from your mobile device.

If you are not required to install an MDM profile when enrolling into Workspace ONE Intelligent Hub, your device is in Registered Mode. In this mode Workspace ONE Intelligent Hub serves as the main entry point for getting your company's resources. This allows you to still access company resources, but you might not have all services like Wi-Fi passcodes and access to internal resources on some system applications as these services might be device management specific features.

VMware makes other productivity applications that your company might have given to you (Boxer, Content, Web, PIV-D, Tunnel, etc.). These apps might also be auto configured for you after you log into Workspace ONE Intelligent Hub. For example, if you logged into Workspace ONE Intelligent Hub and then open your Boxer email application, Boxer will communicate with Workspace ONE Intelligent Hub in the background and seamlessly log you in.

Accessing Other Documents

17

As you configure Workspace ONE integration, you might need to access additional documentation from these documentation centers.

- [VMware Workspace ONE Document Center](#)
 - Hub Services documentation
 - Workspace ONE Integrations
 - Workspace ONE Intelligence
- [VMware Workspace ONE UEM Document Center](#)
 - AirWatch Cloud Connector
 - VMware Workspace ONE UEM Mobile Device Management documentation
 - VMware Workspace ONE UEM Mobile Application Management documentation
 - iOS Device Management documentation
 - Android Platform documentation
- [VMware Workspace ONE Access Documentation Center](#)
 - Workspace ONE Access Administration Guide
 - Managing User Authentication Methods in VMware Workspace ONE Access
 - Setting Up Resources in Workspace ONE Access
 - Integrations - Workspace ONE UEM, Okta, Android Mobile Single Sign-on
 - Configuring AirWatch Provisioning app in Workspace ONE Access