You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
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 Workspace ONE Hub Services  10
   How to Activate Hub Services with Workspace ONE UEM and Workspace ONE Access  11
   Activate Hub Services for Existing UEM Customers  12
   Request a Cloud Tenant in Workspace ONE to Use Hub Services  13
   Reconfiguring Your Workspace ONE Access Cloud Instance to use Hub Services  14

3 Setting Up Hub Services for Your Organization  15
   Using Hub Services Without Enabling Workspace ONE Access  15
   Using Hub Services When Workspace ONE Access Is Integrated  16
      Using Hub Services When Workspace ONE UEM and Workspace ONE Access Are Integrated  17
   Enable Workspace ONE Intelligent Hub Web Browser Experience  18

4 Manage Administrator Roles in Workspace ONE Hub Services (Cloud only)  20
   Add an Administrator Role in Hub Services (Cloud only)  21

5 Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users  23
   Managing Hub Templates  25
   How to Add a Hub Template in Workspace ONE Hub Services and Assign It to Groups  26
   Adding an Onboarding Template and Preparing the Welcome Page for Pre-Hires in Hub Services (Cloud Only)  30

6 Customizing the Workspace ONE Intelligent Hub App Layout  31
   Adding a Custom Tab to Workspace ONE Intelligent Hub  31
   How to Set Up Your Web URL to Display in an iFrame in the Workspace ONE Intelligent Hub Custom tab on the Web Portal  33
   Customize Branding for the Workspace ONE Intelligent Hub App and Web Portal  34
   View Virtual Apps in Workspace ONE Intelligent Hub on Small Screens  37
   Manage Introduction Screens  37

7 Setting up the Workspace ONE Intelligent Hub App Catalog in Hub Services  38
   Customize the Workspace ONE Intelligent Hub App Catalog in Hub Services  39
   Add a Promotions Section to the Catalog App View in Workspace ONE Intelligent Hub  41
   Add Featured Categories as Sections in the Catalog View  41
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Apps That Display in the App Catalog</td>
<td>42</td>
</tr>
<tr>
<td>Enable Hub Catalog for Workspace ONE Customers Updating to Hub Services</td>
<td>43</td>
</tr>
<tr>
<td>Create a Pre-Hire Version of the Hub Catalog for Workspace ONE Intelligent Hub</td>
<td>43</td>
</tr>
<tr>
<td>Migrating Workspace ONE UEM App Catalog Settings to Hub Services</td>
<td>44</td>
</tr>
<tr>
<td><strong>8 Using Hub Notifications Service in Workspace ONE Hub Services</strong></td>
<td>47</td>
</tr>
<tr>
<td>Notifications Types That Can Be Sent from Workspace ONE Hub Services</td>
<td>48</td>
</tr>
<tr>
<td>Setting Up Push Notifications in Hub Services for Workspace ONE Access (On Premises only)</td>
<td>50</td>
</tr>
<tr>
<td>Create Notifications in Workspace ONE Hub Services</td>
<td>51</td>
</tr>
<tr>
<td>Creating Notification Templates in Workspace ONE Hub Services</td>
<td>53</td>
</tr>
<tr>
<td>Creating Custom Notifications in Workspace ONE Hub Services</td>
<td>55</td>
</tr>
<tr>
<td>Change the Branding of Notifications Sent from Workspace ONE Hub Services</td>
<td>59</td>
</tr>
<tr>
<td>Example of How to Create Notifications in Workspace ONE Hub Services That Require Action</td>
<td>60</td>
</tr>
<tr>
<td>Example of How to Create an Informational Notification in Workspace ONE Hub Services</td>
<td>62</td>
</tr>
<tr>
<td>Action Methods That You Can Configure in the Workspace ONE Notifications API</td>
<td>64</td>
</tr>
<tr>
<td>Enable Workspace ONE mobile flows Notification in Hub Services (Cloud Only)</td>
<td>64</td>
</tr>
<tr>
<td>Configure Out-of-Box Connectors for Workspace ONE mobile flows</td>
<td>65</td>
</tr>
<tr>
<td><strong>9 Enabling Access to Workspace ONE People Search</strong></td>
<td>67</td>
</tr>
<tr>
<td>Enable People Service in Hub Services</td>
<td>67</td>
</tr>
<tr>
<td><strong>10 Configuring Workspace ONE Intelligent Hub Employee Self-Service Features in Hub Services</strong></td>
<td>69</td>
</tr>
<tr>
<td>Customize the Employee Self-Service Page for Intelligent Hub</td>
<td>70</td>
</tr>
<tr>
<td>Create Custom Helpful Links in Hub Services</td>
<td>71</td>
</tr>
<tr>
<td><strong>11 Setting up Hub Digital Badge Service in Workspace ONE Hub Services (Cloud Only)</strong></td>
<td>72</td>
</tr>
<tr>
<td>Digital Badge Service Architecture and System Requirements (Cloud Only)</td>
<td>73</td>
</tr>
<tr>
<td>Configure Digital Badge in Hub Services (Cloud only)</td>
<td>74</td>
</tr>
<tr>
<td>Managing the Digital Badge Experience for End Users (Cloud only)</td>
<td>76</td>
</tr>
<tr>
<td>Creating a Health Attestation Return-to-Work Notification in Hub Services (Cloud only)</td>
<td>77</td>
</tr>
<tr>
<td>Employee Experience When They Receive a Health Attestation Notification in Workspace ONE Intelligent Hub App (Cloud only)</td>
<td>79</td>
</tr>
<tr>
<td><strong>12 About MDM Enrollment in Workspace ONE Intelligent Hub</strong></td>
<td>81</td>
</tr>
<tr>
<td>Workspace ONE Intelligent Hub App Mobile Device Management Settings</td>
<td>81</td>
</tr>
<tr>
<td>Enable Intelligent Hub Device Enrollment and Authentication Mode</td>
<td>83</td>
</tr>
<tr>
<td>Enable Unmanaged Enrollment for iOS Devices</td>
<td>84</td>
</tr>
<tr>
<td>Configure Email and Phone Number Contact Information for Intelligent Hub Support Tab</td>
<td>84</td>
</tr>
</tbody>
</table>
Setting Up Hub Services to Support Workspace ONE Intelligent Hub

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**

<table>
<thead>
<tr>
<th>Hub Feature</th>
<th>Availability for Cloud Deployments</th>
<th>Availability for Workspace ONE Access On-Premises Deployments</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Catalog, known as Hub Catalog</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Notifications                | Yes                              | Yes*  
  *Workspace ONE mobile flow is not available for on premises deployments |
| People                       | Yes                              | Yes                                                         |
| Employee Self-Service support | Yes                              | Yes                                                         |
| Digital Badge                | Yes                              | No                                                          |
| Custom Tab                   | Yes                              | Yes                                                         |
| Branding                     | Yes                              | Yes                                                         |
| Templates                    | Yes                              | Yes  
  Requires Workspace ONE Access 21.08 or later |

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.

This chapter includes the following topics:

- 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 Workspace ONE UEM and Workspace ONE Access deployments meet the necessary requirements.

Network Port Requirement for On Premise Workspace ONE Access Deployments

<table>
<thead>
<tr>
<th>Source Component</th>
<th>Destination Component</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE Access host name</td>
<td>signing.awmdm.com</td>
<td>HTTPS</td>
<td>443</td>
<td>Mandatory to launch Hub Services console and to provision certificates for Workspace ONE Notifications service.</td>
</tr>
</tbody>
</table>

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.

- When Workspace ONE UEM is configured with your Hub Services deployment, Workspace ONE UEM must be version 20.08 or later to configure Templates in Hub Services.

- When Workspace ONE Access is configured with your Hub Services deployment, Workspace ONE Access must be version 21.08 or later to configure Templates in Hub Services.

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 9.0 or later.
- Android devices 4.4 or later.
- Windows 10, version 1709.
- macOS 10.12 or later.

**Intelligent Hub App Versions**

To use all the Hub Services features that are released, make sure users update their devices to the latest version of the Workspace ONE Intelligent Hub app. To use Hub templates with the Intelligent Hub app, the version of the Workspace ONE Intelligent Hub app must be 20.08 and later.

**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 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**

![Console Switching](image)

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 16 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

<table>
<thead>
<tr>
<th>Workspace ONE UEM</th>
<th>Workspace ONE Access</th>
<th>Hub Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Activate Hub Services to enable Hub Services features.</td>
<td>- Manage changes in the Identity &amp; Access Management Workspace ONE UEM tab configured to create the trusted relationship with Workspace ONE UEM.</td>
<td>- Manage the Hub Services features.</td>
</tr>
<tr>
<td>- Set up device enrollment and management rules for devices that use single sign-on to the Workspace ONE Intelligent Hub app.</td>
<td>- Configure authentication methods used for single sign-on.</td>
<td>- App Catalog. Customize how apps displays in the app catalog and enable the app rating feature. Review the rating reports.</td>
</tr>
<tr>
<td>- Create and manage UEM user accounts that access Hub Services features.</td>
<td>- Create conditional access policies to control access to resources.</td>
<td>- Enable the Custom tab and configure the URL.</td>
</tr>
<tr>
<td>This includes enabling the Local Basic User accounts for Workspace ONE.</td>
<td>- Enable the compliance check feature to verify that managed devices adhere to Workspace ONE UEM compliance policies.</td>
<td>- Enable People when UEM is integrated with Workspace ONE Access.</td>
</tr>
<tr>
<td></td>
<td>- Map Identity Manager Domains to Customer Organization Groups in Workspace ONE UEM.</td>
<td>- Create and send Notifications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Manage Help and Support page content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Use Digital Badge to manage employee access to physical spaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Manage the Hub Services system settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Customize branding.</td>
</tr>
</tbody>
</table>

VMware, Inc.
Activating Workspace ONE Hub Services

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, an enhanced notification with VMware Workspace ONE® mobile flows, 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**

<table>
<thead>
<tr>
<th>Hub Feature</th>
<th>Available with Workspace ONE UEM</th>
<th>Available with Workspace ONE Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>App catalog</td>
<td>Yes For Workspace ONE UEM apps</td>
<td>Yes Unified app catalog with SSO and conditional access</td>
</tr>
<tr>
<td>Customize Branding</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notifications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Basic corporate communication</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
VMware Workspace ONE Hub Services Documentation

<table>
<thead>
<tr>
<th>Hub Feature</th>
<th>Available with Workspace ONE UEM</th>
<th>Available with Workspace ONE Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifications</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrate with Workspace ONE mobile flows to receive notifications from business apps that are configured in mobile flows. (Cloud only) Workspace ONE Access must be integrated with Workspace ONE UEM and the mobile flows service must be configured in your Workspace ONE UEM environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Tab</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Employee Self-Service Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>People</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Digital Badge</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cloud deployments only</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- **How to Activate Hub Services with Workspace ONE UEM and Workspace ONE Access**
- **Activate Hub Services for Existing UEM Customers**
- **Request a Cloud Tenant in Workspace ONE to Use Hub Services**
- **Reconfiguring Your Workspace ONE Access Cloud Instance to use Hub Services**

### 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 Intelligent Hub app.

**Existing Cloud Workspace ONE UEM Customers**

If you are an existing Workspace ONE UEM customer, you receive an email that includes a link to your Workspace ONE Access cloud tenant. In the Workspace ONE UEM console Groups & Settings > Intelligent Hub pages, you add the cloud tenant URL and the tenant admin user name and password to activate Hub Services. See Activate Hub Services for Existing UEM Customers.
If you did not receive an email with a link to your Workspace ONE Access cloud tenant, you can request a tenant from the Workspace ONE UEM console, Intelligent Hub pages. See Request a Cloud Tenant in Workspace ONE to Use Hub Services.

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, Catalog > Hub Configuration page to configure the layout of the catalog. You can add your logo and company branding and also enable other Hub Services functionality.

To use the 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 UEM Customers

Existing Workspace ONE UEM customers who want to use Hub Services must enter their Workspace ONE Access cloud tenant URL and the admin name and password to activate Hub Services.

If you do not have a cloud tenant, you can request one from the Workspace ONE UEM console. Currently, this option is available only to cloud UEM customers. See Request a Cloud Tenant in Workspace ONE to Use Hub Services.

Prerequisites

Workspace ONE Access cloud tenant URL and the admin name and password to access the tenant. Your cloud tenant URL was sent in an email. You can file a support ticket if you do not know the URL that was assigned.

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 Cloud Tenant URL as https://myco.vmware.com. Enter the admin user name and the password that can access this tenant.
3 Click **TEST CONNECTION** to confirm that Workspace ONE UEM and Workspace ONE Access are communicating securely.

If the connection fails, check that the source of authentication for Intelligent Hub is Workspace ONE Access.

- Navigate to the Configurations > Intelligent Hub page and click **Intelligent Hub**.
- Scroll to the section labeled Source of Authentication and click **Configure**.
- In the Devices & Users > General > Enrollment page, scroll to **Source of Authentication for Intelligent Hub** and make sure that Workspace ONE Access is selected.
- Click **Save**.
- Retest the connection.

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**

Configure the Hub services. You can customize the Hub Services features and configure how you want the Intelligent Hub to look and feel in the Branding page. See Chapter 3 Setting Up Hub Services for Your Organization.

**Request a Cloud Tenant in Workspace ONE to Use Hub Services**

To use Hub Services, you can request a new cloud tenant if you do not have one.

**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, click **REQUEST CLOUD TENANT**.

3 Accept the terms of service and click **Next**.

4 The Administrator Details page is prefilled with your URL, user name, and password. Verify that the information is correct and click **Next**.

5 In the Pick Data Center Location page, select the data center nearest to your organization and click **Next**.

   A tenant name is automatically created for you. You cannot request a specific name.

6 Click **Save**.
Results

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

What to do next

Return to the Hub Configuration page to configure Hub Services. See Activate Hub Services for Existing UEM Customers

Reconfiguring Your Workspace ONE Access Cloud Instance to use Hub Services

If you originally configured your Workspace ONE Access tenant for the Workspace ONE App and now are activating Hub Services to use the Workspace ONE Intelligent Hub app, you must update some of the Workspace ONE UEM settings.

After you activate Hub Services with the new cloud instance, you must reconfigure several components in the Workspace ONE UEM console.

Table 2-1. Workspace ONE Access Components to Reconfigure

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Services</td>
<td>Active Directory is reset to be deactivated. You must reactivate Active Directory Basic. The user mapping is reset to the default values. You must reconfigure the user attributes to be mapped.</td>
<td>See Directory Integration with VMware Workspace ONE Access.</td>
</tr>
<tr>
<td>Directory Services with Basic User Sync</td>
<td>If you configured Local Basic User sync previously, you must re-enable Basic User Sync.</td>
<td>See Sync Users and Groups from Workspace ONE UEM Directory to Workspace ONE Access Directory.</td>
</tr>
<tr>
<td>Access Policies</td>
<td>Access policies that manage single sign-on are no longer available. You must reconfigure the default access policy.</td>
<td>Edit the Default Access Policy in Workspace ONE Access.</td>
</tr>
<tr>
<td>Active Directory Basic and SaaS and Virtual App Support in Workspace ONE UEM Console.</td>
<td>Web apps and virtual apps are not accessible from the UEM console. You must reconfigure the default access policy, and any other policies created for specific web apps. You might have to update the Workspace ONE UEM settings in the Workspace ONE Access console. Review the Workspace ONE UEM settings page in the Workspace ONE Access console.</td>
<td>See the Directory Service Integration guide in the VMware Workspace ONE UEM doc center.</td>
</tr>
</tbody>
</table>
Setting Up Hub Services for Your Organization

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.

This chapter includes the following topics:
- Using Hub Services Without Enabling Workspace ONE Access
- Using Hub Services When Workspace ONE Access Is Integrated

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 Intelligent Hub app on iOS and Android devices. The Notifications functionality is enabled by default. Notifications about new apps that are available are automatically sent to users. 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 > Hub Configuration 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 Notifications through Workspace ONE Experience Workflows.

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.
Workspace ONE cloud tenants can configure VMware Workspace ONE™ Experience Workflows® business system integration packs in the Hub Services console. Workspace ONE Experience Workflows is a framework built within the Hub Services platform that connects between different business systems to orchestrate microapps that enable end users to quickly complete tasks from the Workspace ONE Intelligent Hub app. The Workspace ONE Experience Workflows Add-On license is required. See the [VMware Workspace ONE Experience Workflows Configuration Guide](#).

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

[Diagram showing the integration of 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, additional Hub Services features can be configured.

- **People.** 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](#).

- **Notifications through Workspace ONE mobile flows.** The Notifications functionality is enabled by default and when Workspace ONE Access is integrated, you can enable the mobile flows integration with Hub Services to receive notifications from business apps that are configured in mobile flows.

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.

## Enable Workspace ONE Intelligent Hub Web Browser Experience

Existing cloud tenant Workspace ONE UEM customers and Workspace ONE Access customers moving to Hub Services must enable the web browser experience in Hub Services.

**Procedure**

1. Navigate to the Hub Services console Home page.
2. Click **System Settings**.
3. Enable **Hub Browser Experience**
4. Click **Save**.
Results

The web portal displays the Favorites and App tabs. In the App tab, users see the Promotions, New Apps and the Categories list. The People, Notifications, For You, and Employee Self-Service pages display as separate tabs, if they are enabled.

Manage Administrator Roles in Workspace ONE Hub Services (Cloud only)

Hub Services uses role-based access control (RBAC) to manage who can access the services in the Hub Service console and what settings administrators can see and change in the console.

Five predefined administrator access roles can be configured in the Hub Services console Admin Role 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.

- **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 Global Settings tab.

- **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 Notifications List and the Global Settings tab.

- **Notification Auditor.** The notification auditor role has read-only permissions to view the Notifications List tab and Global Settings tab in the Notifications page.

You assign roles to Workspace ONE Access user groups. You can assign more than one role to a group.

When a group is assigned more than one role, the behavior of the roles applied is additive. For example, if an administrator is assigned two roles, one as 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.

You see the list of the current admins groups and their roles, change a role, and remove roles from the 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 to select the Manage Hub Experience link.
Hub Services Super Admin Roles

Workspace ONE Access super administrators are automatically super admins in the Hub Services console. The Workspace ONE Access super administrator initially configures the Hub Services super admin role and assigns Workspace ONE Access groups to the role. Members of the group can access and manage all features and functions in the Hub Services console. This includes adding new groups as super admins and adding groups to any of the other admin roles. Members of the Hub Services super admin group do not have access permissions to the Workspace ONE Access console.

Workspace ONE Access non-super administrators are Hub Services auditor admins. They can become Hub Services super admins if they are in a user group that is assigned the super admin role.

Create Roles to Manage the Notifications Service

You can delegate limited access to user groups to access only the Notifications Service pages in the Hub Service Console to manage, create, and send notifications. For example, you can assign the notification creator role to the HR group so that they can create and send HR notifications, and grant the same role to the Support Team group so they can create and send support notifications. You can assign another group to the notifications admin role that gives members of that group access to all settings in the Notifications Service page.

This chapter includes the following topics:

- Add an Administrator Role in Hub Services (Cloud only)

Add an Administrator Role in Hub Services (Cloud only)

To assign a role in the Hub Service console, you must be a Workspace ONE Access super administrator or a Hub Services super admin who can access and manage all features and functions in Hub Services.

Prerequisites

Identify the 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.
4. Enter the Workspace ONE Access group name for this new admin role.
5. Select the role to assign.
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 new permissions and how to log into the Hub Services console from the Manage Hub Experience link on the Workspace ONE Intelligent Hub portal.
Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users

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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Versionable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App Catalog</td>
<td>Yes</td>
<td>Create versions of the Hub catalog that are configured with different sets of apps and sections to promote.</td>
</tr>
<tr>
<td>Branding</td>
<td>Yes</td>
<td>Create different versions of branding for Workspace ONE Intelligent Hub to customize the logo and branding for different sets of users.</td>
</tr>
<tr>
<td>Custom Tab</td>
<td>Yes</td>
<td>Create versions of the custom tab, each with a different label, URL, and position on the navigation bar.</td>
</tr>
<tr>
<td>Employee Self-Service</td>
<td>Yes</td>
<td>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. If you do not require a global setting for employee self-service, you can deactivate the global setting. 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.</td>
</tr>
<tr>
<td>Feature</td>
<td>Versionable</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  

**Note** The Workspace ONE mobile flows URL set in System Settings is set as a global value and cannot be changed.  

| 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.  

| Digital Badge    | No          | You do not create versions of the Digital Badge setting. To manage which groups can use Digital Badge, you deactivate Digital Badge as a global setting and enable the Digital Badge setting in templates that can use the feature.  

To use the Digital Badge feature in templates, the Digital Badge settings must be configured in the Digital Badge page in Hub Services.  

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.  

This chapter includes the following topics:  

- Managing Hub Templates  

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

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

Hub Templates that you create are listed on the Templates page in a prioritized order with the highest priority listed first.

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 Hub Template in Workspace ONE Hub Services and Assign It to Groups

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 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 Intelligent Hub app for iOS, Android, Mac, and Windows devices. 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 Intelligent Hub experience on iOS, Android, Mac, and Windows Intelligent Hub apps is not available. Only the web browser experience is available.
You can copy a template, change the name of the template, and change feature 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.

   ![Branding Configuration](image1)

   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.

   ![App Catalog Configuration](image2)

   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**.

   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.
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.

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, Digital Badge, 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

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.

This chapter includes the following topics:

- 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 Web Portal
- View Virtual Apps in Workspace ONE Intelligent Hub on Small Screens
- Manage Introduction Screens

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 uses 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 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


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 Web Portal**

You can use your organization's logo in the Workspace ONE Intelligent Hub app and 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 on 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.

You cannot deactivate branding.

**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 exact 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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logos</td>
<td><strong>Organization Logo.</strong> Click <strong>Upload</strong> 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. <strong>Mobile App icon.</strong> You can change the color of the Workspace ONE Intelligent Hub app icon that displays on devices.</td>
</tr>
<tr>
<td>Web Browser</td>
<td><strong>Organization Name.</strong> Enter the organization name to use as the title that displays in the browser tab. The default name is VMware. <strong>Product Name.</strong> Enter the text that displays after the organization name in the browser tab. The default name is Intelligent Hub. <strong>Favicon.</strong> 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 <strong>Upload</strong> to upload a new image to replace the current favicon.</td>
</tr>
<tr>
<td>Navigation Bar</td>
<td>You can configure the appearance of the web browser navigation bar. <strong>Background Color.</strong> 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. <strong>Font &amp; Icon Color.</strong> Depending on your background color, select either Black or White for the text color.</td>
</tr>
<tr>
<td>Tab Bar (Mobile)</td>
<td>You can configure the appearance of the tab bar on iOS and Android devices. <strong>Font &amp; Icon Color.</strong></td>
</tr>
<tr>
<td>Content</td>
<td><strong>Accent Color.</strong> 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. <strong>Advanced Content Branding Options.</strong> <strong>Background Color.</strong> 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. <strong>Note.</strong> Do not select the same hex value for the accent color and background color. The app pages might not display correctly. <strong>Font &amp; Icon Color.</strong> Depending on your background color, select either Black or White for the text color.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Tab Bar (Mobile)     | **Font & Icon Color.**  
  - Select **Use Default branding** to display the Intelligent Hub app text and icon colors that you configured for the Content.  
  - Select **Same as Navigation Bar** to use the font and icon color configured for the Navigation Bar.                                                                                                                                                     |
| Dark Mode            | 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.  
  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.  
  - **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.  
  - **Accent Color.** The accent color is the highlight color that is applied to links and active areas. Use lighter tones for better visibility on dark mode screens.  
  **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. |
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 Introduction Screens

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Apps</td>
<td>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.</td>
</tr>
<tr>
<td>Recommended</td>
<td>Preferred applications that you categorized as recommended in the catalog are displayed in the Recommended section.</td>
</tr>
<tr>
<td>Category List</td>
<td>The Categories section displays a list of all 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.</td>
</tr>
<tr>
<td>Promotions</td>
<td>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.</td>
</tr>
<tr>
<td>Updates</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The ability to display the Updates section is only available on iOS devices with Workspace ONE Intelligent Hub app version 21.06 and later.</td>
</tr>
<tr>
<td>Custom</td>
<td>You can create custom category sections.</td>
</tr>
</tbody>
</table>

The Favorites tab is enabled as a separate tab that displays apps that users mark as a favorite. When Favorites is enabled in the Hub console App Catalog page, 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 no 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.

**Note** Currently the Web Links feature is supported in the Hub Web portal view.
This chapter includes the following topics:

- 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
- Managing Apps That Display in the 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, you can enable the ability to use the web to access apps in Workspace ONE Intelligent Hub from 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 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 disabled, 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.

**Note** Currently, the Show Web Links feature is available in the Hub Web portal view only.

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 disabled, 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.

**Note**  Currently, the Show Web Links feature is available in the Hub Web portal view only.

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.

Managing Apps That Display in the 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, and the Horizon Cloud Administration console.

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. You manage the UEM catalog from the Workspace ONE UEM console, Apps & Books > Applications > Applications Settings pages. See the Application Management Life-Cycle guide in the [Workspace ONE UEM Documentation](https://www.vmware.com/support/ces/vmware-workspace-one-uem.html) center.

In the Workspace ONE Access console, you configure, manage, and entitle uses to web apps and virtual apps. Some web application can be added 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](https://www.vmware.com/support/ces/vmware-workspace-access.html) for information about setting up these resources in Workspace ONE Access.

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 as well as sync settings. See [Providing Access to VMware Horizon Cloud Services Desktops and Applications](https://www.vmware.com/support/pubs/VMware-Horizon-Cloud-PUB-00000269A.html).

(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](https://www.vmware.com/support/pubs/VMware-Horizon-Cloud-PUB-00000269A.html).
Enable Hub Catalog for Workspace ONE Customers Updating to Hub Services

After you activate Hub Services in the UEM console, you can configure the catalog settings to enable the Hub Catalog for iOS, Android, and macOS devices.

**Note**  The Hub Catalog is automatically enabled for new cloud-tenant customers.

**Procedure**

1. In the Workspace ONE UEM console, select your Global > customer level organization group, and navigate to the Groups & Settings > All settings > Apps > Workspace ONE > AirWatch Catalog > General page.
2. Click Publishing. Make sure that the current setting is Override. In the Platforms section, enable Intelligent Hub Catalog (iOS), Intelligent Hub Catalog (Android), and Intelligent Hub Catalog (macOS) options to publish the Hub catalog to these devices.

   No other changes on this page are required.
3. (Optional). Deactivate the legacy catalogs for iOS, Android, and macOS to decommission the AirWatch Legacy catalog.
4. Click Save.

**Results**

The Hub Catalog is enabled.

**What to do next**

Go to the Hub Services console Customization page to customize the catalog page view to add new sections such as Promotions, Favorites, and New Apps. See Adding a Custom Tab to Workspace ONE Intelligent Hub.

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.
   - Delete the **New Apps**, **Recommended**, and **Category List** sections.
   - Deactivate the **Favorites** Tab.
   - Leave **Show Virtual Apps on Devices** and **Enable App Ratings** deactivated.

6. In the **Promotions** row, click to expand the row.
   - Leave the **Display the Promotions section** enabled.
   - 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 Hub 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 notifications 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 notifications on their iOS, Android, macOS, and Windows devices and in the web portal from a browser.
- Users receive new app notifications about web and virtual apps.
- Workspace ONE mobile flows can be enabled and notifications from mobile flows configured business systems can be received. (Cloud only)

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.

This chapter includes the following topics:
Notifications Types That Can Be Sent from Workspace ONE Hub Services

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

Create Notifications in Workspace ONE Hub Services

Creating Notification Templates in Workspace ONE Hub Services

Creating Custom Notifications in Workspace ONE Hub Services

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

Enable Workspace ONE mobile flows Notification in Hub Services (Cloud Only)

Configure Out-of-Box Connectors for Workspace ONE mobile flows

Notifications Types 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.
A New App notification to inform users about new apps that are granted to them is available with the Workspace ONE Intelligent Hub app.

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. If you do not want employees to receive the weekly notification, you can deactivate the New App Notifications setting in the Notifications Settings page.

The new app notification message template cannot be modified.

You can create custom notifications and set a notification priority in the Notification wizard in the Hub Services console or with the Notification APIs.

When you use Notification wizard, two notification types are listed.

- **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.

- **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.

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](https://code.vmware.com/apis/402#/Notifications). The Notifications Service reference guide is available from the Documentation tab on that page.

When you create a notification, you can set the priority of the notification as either Standard, High-Priority, or Urgent.

- **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.

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](https://code.vmware.com/apis/402#/Notifications).

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 notification, and it displays at the top of the For You page until the notification expires.

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.

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 Notifications Guide in the Workspace ONE Notifications Service API Documentation tab, and the hero card schema for more information.

*Note: mobile flow configuration is available only for cloud tenant deployments.

You can enable Workspace ONE mobile flows integration with Hub Services to receive notifications from business apps that are configured in mobile flows. Workspace ONE Access must be integrated with Workspace ONE UEM and the mobile flows service must be configured in your Workspace ONE UEM environment.
How 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 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 History. 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.

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,
   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.

**Create Notifications in Workspace ONE Hub Services**

You can use the Custom Notification wizard 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 and click New and then click Create Notification.
2. Enter the name of the notification.
   
   This name displays in the Notification list on the Notifications page.
3. Select the target audience.

   You can target custom notifications to specific audiences or you can send the notification to all employees in your organization. You can assign the following audience types.

<table>
<thead>
<tr>
<th>Audience Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Employees</td>
<td>Notifications can be sent to all employees listed as users in the Workspace ONE Access service.</td>
</tr>
<tr>
<td>All Devices</td>
<td>Notifications can be sent to all devices configured in your Workspace ONE UEM environment, regardless of organization groups.</td>
</tr>
</tbody>
</table>
### Audience Types

<table>
<thead>
<tr>
<th>Audience Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Group</td>
<td>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.</td>
</tr>
<tr>
<td>Smart Group</td>
<td>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.</td>
</tr>
<tr>
<td>Platform</td>
<td>You can select a specific platform type to send a notification. The platforms are iOS, Android, macOS, and Windows.</td>
</tr>
<tr>
<td>Users Group</td>
<td>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.</td>
</tr>
</tbody>
</table>

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**, **High-priority**, **Urgent**.
   - If you implemented Hub Services Digital Badge access, **Return to Work** is listed as a priority option.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Use the default image, Intelligent Hub or add your company logo.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the title that describe the notification topic. The title displays in the notification heading.</td>
</tr>
<tr>
<td>Subtitle (optional)</td>
<td>The subtitle appears above the title.</td>
</tr>
</tbody>
</table>
You can add either a video or an image to the notification card.

To display an image in the notification banner, make sure you include the full link address. Example of an image URL, https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078f206641.png. The image must be either a jpg or png file and the aspect ratio of the image is 4:3.

Description
Type the message.

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)
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.

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.

9 Click Next to see a summary of the notification.

10 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 8-1. Actions Available from the Notifications List

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.

   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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>By default, the Intelligent Hub 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</td>
</tr>
<tr>
<td>Title</td>
<td>Enter a title that describes the notification topic</td>
</tr>
<tr>
<td>Subtitle</td>
<td>Optional</td>
</tr>
<tr>
<td>Media Type (optional)</td>
<td>You can add an image or video to the banner section of the notification. Add the complete link address of the image. For example, <a href="https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png">https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png</a>. To display a video in the notification banner, paste the video embedded code</td>
</tr>
<tr>
<td>Description</td>
<td>Type the notification message in the <strong>Description</strong> box.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Additional Details</td>
<td>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.</td>
</tr>
<tr>
<td>Links (optional)</td>
<td>Add the link title that displays in the notification and the complete link URL. The notification can include up to 10 links.</td>
</tr>
</tbody>
</table>

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

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.

**Creating Custom Notifications in Workspace ONE Hub Services**

The Custom Notification wizard 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 custom notification can be Actionable and Informational. See **Notifications Types 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**.
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.

Selecting the Target Audience

You can target custom notifications to specific audiences or you can send the notification to all employees in your organization. You can assign the following audience types.

<table>
<thead>
<tr>
<th>Audience Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Employees</td>
<td>Notifications can be sent to all employees listed as users in the Workspace ONE Access service.</td>
</tr>
<tr>
<td>All Devices</td>
<td>Notifications can be sent to all devices configured in your Workspace ONE UEM environment, regardless of organization groups.</td>
</tr>
<tr>
<td>Organization Group</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Audience Types

<table>
<thead>
<tr>
<th>Audience Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Group</td>
<td>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.</td>
</tr>
<tr>
<td>Platform</td>
<td>You can select a specific platform type to send a notification. The platforms are iOS, Android, macOS, and Windows.</td>
</tr>
<tr>
<td>Users Group</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

### 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

<table>
<thead>
<tr>
<th>API</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>Use GET to retrieve data from a specified resource. The data is not modified. Enter the URL of the resource that supplies the data.</td>
</tr>
<tr>
<td>POST</td>
<td>Use POST to send data to a specified URL to insert data in a resource. Enter the URL where the data is sent.</td>
</tr>
<tr>
<td>PUT</td>
<td>Use PUT to send data to a specified URL to update a resource. Use PUT when user can only send the data one time.</td>
</tr>
<tr>
<td>API</td>
<td>Task Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PATCH</td>
<td>Use PATCH to allow users to modify their data on the resource.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Use Delete to let the user delete data from the specified URL.</td>
</tr>
</tbody>
</table>

- **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 View more section of the notification.

- To display an image in the notification banner, make sure you include the full link address. Example of an image URL, [https://www.mozilla.org/media/img/firefox/new/desktop/hero-mr1.c078ff206641.png](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, you paste the video embed code in the content page when you configure the notification.

- 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.
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.

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.

**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 to 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.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Use the default image, Intelligent Hub or you can add your own image for this notification.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the title as <strong>Security Training Required</strong>.</td>
</tr>
<tr>
<td>Subtitle (optional)</td>
<td>To highlight the completion date, enter the subtitle <strong>Must be completed by August 1</strong>.</td>
</tr>
<tr>
<td>Media Type (optional)</td>
<td>You can add an image or video to the banner section of the notification.</td>
</tr>
</tbody>
</table>
| 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.                                                                                               |
This notification is created with two actions, Completed and Training Required.

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

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

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.

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

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 see a summary of the notification.

9. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Use the default image, Intelligent Hub or add your company logo.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter the title as <strong>Company Quarterly Meeting</strong>.</td>
</tr>
<tr>
<td>Subtitle (optional)</td>
<td>To highlight the meeting start time, enter the subtitle <strong>Starting at 10:00 a.m. PST.</strong></td>
</tr>
<tr>
<td>Media Type (optional)</td>
<td>You can add either a video or an image to the notification card.</td>
</tr>
<tr>
<td>Description</td>
<td>Type the message. The quarterly meeting will be starting in a few minutes, hope you can attend.</td>
</tr>
<tr>
<td>Links (optional)</td>
<td>Your notification can include up to 10 links.</td>
</tr>
<tr>
<td>Additional Details</td>
<td>Click <strong>Add Details</strong> to add a feature, fact, or other item that you want to call out in the notification. Enter as a label and the description.</td>
</tr>
<tr>
<td>Attachments</td>
<td>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.</td>
</tr>
</tbody>
</table>
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](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 hardcoded 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.

**Enable Workspace ONE mobile flows Notification in Hub Services (Cloud Only)**

The Workspace ONE mobile flows service processes the notification workflow from other business apps such as Salesforce and delivers them to apps that integrate with Workspace ONE mobile flows. You must enable mobile flows in the Hub Services console to display notifications from mobile flows-configured business systems within Workspace ONE Intelligent Hub.

When the mobile flows service is integrated with Hub Services, users receive notifications in their web portal and Workspace ONE Intelligent Hub app on their devices. Users can act on the notification directly from within the portal or app. They do not need to navigate to another business app to respond to the notification.
Prerequisites

- Workspace ONE mobile flows server provisioned with Workspace ONE UEM. See the Workspace ONE mobile flows guide.
- Workspace ONE mobile flows connectors to the business apps configured. See Configure Out-of-Box Connectors for Workspace ONE mobile flows.
- Hub browser experience enabled in the Hub Services console
- Notifications enabled in the Hub Services console

Procedure

1. Navigate to the Hub Services console Home page.
2. Click Notifications and select the Settings tab.
3. Select Enable Workspace ONE mobile flows.
4. Click SAVE.

Results

The mobile flows host URL is added to the Hub Services System Settings page. You can view and update the mobile flows URL from the Settings page.

Users can now receive notifications in Intelligent Hub that come from the configured business systems and pass through the mobile flows service. Users receive notifications from the configured business systems. They can deactivate receiving notifications from the Intelligent Hub app user’s Account > Device > Preferences screen.

Note

- You cannot deactivate the mobile flows integration once it is activated. To remove the integration and not receive notifications through mobile flows, in the UEM console, navigate to Content > Mobile flows > My Flows and remove or deactivate the configured connectors for Intelligent Hub.

Configure Out-of-Box Connectors for Workspace ONE mobile flows

To use the Workspace ONE mobile flows service with Hub Services, you must configure a mobile flows out-of-the-box (OOTB) connector component for each business app that supports approval workflows. The connector fetches user-specific information from the business system. Out-of-the-box connectors are connector templates with pre-configured information that you can add directly to your mobile applications workflow.

The connectors retrieve user-specific information from the business systems and send responses back to their portal and to the Intelligent Hub app on their devices.

For the list of available notification connectors, see the mobile flows out of the box connector list.
Prerequisites

Workspace ONE UEM console version 1905 or later to use the OOTB connectors. For more information about mobile flows, see the Workspace ONE mobile flows documentation.

The Hub Browser must be enabled. If the Hub Browser setting is not enabled, go to the Catalog > Hub Configuration > Customization page and enable Hub Browser. See Enable Workspace ONE Intelligent Hub Web Browser Experience.

Procedure

1. In the Workspace ONE UEM console, navigate to Content > Mobile flows > Catalog.
2. Click ADD on the OOTB connector that you want to configure.
3. On the page that appears, enter the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base URL</td>
<td>Enter the public URL for the SaaS application/business system you are configuring.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select the user authentication type. Depending on the authentication type selected, corresponding configurations might need to be defined.</td>
</tr>
</tbody>
</table>

4. Click Save.

The connector is added to the My Flows tab on the Mobile Flows page. Allow up to 15 minutes for the changes you make to the mobile flows connectors to appear in the Hub Services console.
Enabling Access to Workspace ONE People Search

When Hub Services is fully integrated with Workspace ONE Access, you can enable access to the People service to let users search for their colleagues and view user details and organization charts directly from the Workspace ONE Intelligent Hub app or web portal.

To use this service, the People Search feature must be enabled in the Workspace ONE Access console, Catalog > Settings page. You then select the user profile attributes that you want to display in the search results. The attributes are mapped to the corresponding Active Directory attributes. The Workspace ONE Access directory is updated with this information when the directory syncs to the Active Directory.

**Note** Make sure that Workspace ONE Access is configured as the authentication method in the Workspace ONE UEM console.

When you enable access to the People service, the People link displays in the Workspace ONE Intelligent Hub app and the web 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.

- Users profile details
- A 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.

This chapter includes the following topics:

- Enable People Service in Hub Services

Enable People Service in Hub Services

After you enable People Search in the Workspace ONE Access console, you can enable the People feature in the Hub Services console.
Prerequisites

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

Procedure

1. Navigate to the Hub Services console Home page.
2. Click **People** and enable **People by default**.
3. Click **Save**.

Results

The People tab is added to the Intelligent Hub app, user 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 right away after you enable the People feature, you can push the changes. 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`. Before you run this command to push the change, make sure that you are logged into the web portal.
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.

The option to view the self-service tab in the browser is on by default in the global setting. You can deactivate 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 the specific group.

**Change the Self-Service Tab Name**

The tab that displays in the Workspace ONE Intelligent Hub app displays as Support in the navigation bar. You can change the label in the Employee Self-Service page. The new name displays in the navigation bar when the app view is refreshed.

**Manage Contact Information**

When Workspace ONE UEM is configured to enroll device 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 Devices > Devices Settings > Devices & Users > General > Enrollment > Customization tab.

---

**Note** The Customization tab shows an example email and phone numbers. If you do not change the example settings, this information display in the Contacts section. See Configure Email and Phone Number Contact Information for Intelligent Hub Support Tab.

**Self-Service Options for User Device Management**

You can enable device self-service to display the My devices section in the self-service tab in the Workspace ONE Intelligent Hub app. My devices section provides detailed information about the user’s devices. By default, users can add devices and install profiles for devices that are enabled. Users can also click Sync to sync all profiles to the device.
You can deactivate these options in the Employee Self-Service page.

## Add Helpful Links

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 reaching out to your support service. These links are displayed in the **Helpful Resources** section in the self-service tab.

This chapter includes the following topics:

- Customize the Employee Self-Service Page for Intelligent Hub
- Create Custom Helpful Links in Hub Services

### Customize the Employee Self-Service Page for Intelligent Hub

You can set up an employee self-service page for employees to access in Intelligent Hub.

You can create different versions of the employee self-service page.

### Add a Global Employee Self-Service Tab

The global employee self-service tab is displayed in the Intelligent Hub app. When you create a template, you can also add the custom tab.

1. Navigate to the Hub Services console Home page.
2. Click **Employee Self-Service**.
3. To set up a global employee self-service tab that displays in the Intelligent Hub app, enable **Enable Employee Self-Service**.
4. Enter the name to display on the tab. The default label is **Support**.
   
   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.
5. Enable Device Self-Service to let users manage their own devices in Intelligent Hub and add optional profiles to their Employee Self-Service page.
6. Add Helpful links for employees to access links and to other resources. See **Create Custom Helpful Links in Hub Services**.
7. Click **Save**.

### Add Version of Employee Self-Service Tab

1. Navigate to the Hub Services console Home page.
2. Click **Employee Self-Service**.
3  To set up a global employee self-service tab that displays in the Intelligent Hub app, enable **Enable Employee Self-Service**.

4  Enter the name to display on the tab. The default label is **Support**.
    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.

5  Enable Device Self-Service to let users manage their own devices in Intelligent Hub and add optional profiles to their Employee Self-Service page.

6  Add Helpful links for employees to access links and to other resources. See Create Custom Helpful Links in Hub Services.

7  Click **Save**.

### Create Custom Helpful Links in Hub Services

In the Hub Services Employee Self-Service page, you can add help links to direct users to internal or external sites and knowledge base articles for self-service help.

You can add up to 10 links to direct users to resources. Users can find these links in the Support tab, Helpful Links section.

**Procedure**

1  Navigate to the Hub Services console Home page.

2  Click **Employee Self-Service**.

3  In the Helpful Links section, click **Add**.

4  Click **ADD SECTION** and begin typing the title to the link.

5  Tab to the **Link** line and enter the full URL address.

6  Continue to add up to 10 links to the list.

7  Click **SAVE**.

    Note: Click **X** to remove a helpful link from the list.
The Digital Badge service is a component of Hub Services that can be integrated with Physical Access Control Systems (PACS) to allow the Workspace ONE Intelligent Hub app on mobile devices to act as a digital badge. When the Digital Badge service is integrated with PACS, the Workspace ONE Intelligent Hub app can work like a physical employee badge and provide a hands-free access to unlock doors.

The Digital Badge service can also be used along with Health Attestation surveys in the Workspace ONE Intelligent Hub app to manage users’ temporary access to specific buildings based on survey answers. The Health Attestation survey can control the access for physical badges only, so deploying the Digital Badge feature is not a mandatory step for this use case.

To use the Digital Badge service, your organization must deploy the following access control infrastructure.

- To connect and work with the Digital Badge service, deploy the Physical Access Control System (PACS) by Software House C•CURE 9000 version 2.8.
  - Because PACS is deployed on-premises, a best practice is to configure a reverse proxy so that the C•CURE system is not exposed externally.
  - Use the Nginx service or some other service to create an IP-based or domain-based allow list for Hub Services access to C•CURE.
- For a digital ID in Workspace ONE Intelligent Hub app, deploy the following.
  - The SaaS tenant in the HID Origo Management Portal used as a mobile badge management service with enough purchased mobile user licenses to cover the number of users that use this service.
  - Door Badge Reader that is a HID Bluetooth capable reader, either the HID Signo iCLASS SE reader or the multiCLASS SE reader.

This chapter includes the following topics:

- Digital Badge Service Architecture and System Requirements (Cloud Only)
- Configure Digital Badge in Hub Services (Cloud only)
- Managing the Digital Badge Experience for End Users (Cloud only)
- Creating a Health Attestation Return-to-Work Notification in Hub Services (Cloud only)
Digital Badge Service Architecture and System Requirements (Cloud Only)

The Digital Badge service is configured in the Hub Service console to communicate with the HID Global Origo Management Portal service and to communicate with your on-premises C•CURE physical access control system.

Figure 11-1. Hub Services Digital Badge Architecture Flow

If the PACs system is deployed within your internal network and is not normally exposed publicly, the recommended approach is to place a reverse proxy in the DMZ. The reverse proxy allows the Digital Badge service to be placed on an IP-based or domain-based allow list and connect securely to the internal PACs. See the SaaS IP address ranges used for network configuration KB article.

External Systems Required to Be in Place in Your Organization

To use the Digital Badge service, your organization must deploy the following access control infrastructure.

- Software House C•CURE 9000 version 2.8 Physical Access Control (PACs) service
- For digital IDs
  - SaaS tenant in the HID Origo Management Portal
  - HID Signo, iCLASS SE or multiCLASS SE Bluetooth capable readers
VMware Workspace ONE Platform Component

If Workspace ONE UEM is configured, Workspace ONE UEM must be version 2008 or later to configure Hub Templates in Hub Services.

Mobile Devices

- Android version 4.4 or later with Workspace ONE Intelligent Hub app 20.05 or later
- iOS version 11 or later with Workspace ONE Intelligent Hub app 20.05.1 or later

Configure Digital Badge in Hub Services (Cloud only)

You configure the Digital Badge service, adding HID Global Origo setting and C•CURE setting details in the Hub Services console. After the Digital Badge service is configured, you enable Digital Badge in Hub Services.

Configure Digital Badge Service with HID Origo Management Portal Integration Settings

You can configure Digital Badge as a production or a non-production instance. Select Non-production when you are setting up a Digital Badge service in a preview environment or for other non-production purposes. Select Production to deploy the Digital Badge service in the Workspace ONE Intelligent Hub app to all users.

Prerequisites

Make sure that you have the required HID Origo SaaS Tenant configuration settings.

- Client ID and Client Secret. OAuth credentials generated in the Origo portal. These settings are used to authorize the connection from the Hub Digital Badge service.
- Application ID. The unique Origo tenant ID.
- Part Number. The active part number with the subscription type reference. The part number is used to confirm that there are available mobile user licenses.

Procedure

1. Navigate to the Hub Services console Home page.
2. Click Digital Badge and select Yes for Configure Digital Badge.
3. Enter the HID Origo Client ID, Client Secret, App ID, and Part Numbers.
4. Test the connection.

Configure C•CURE Settings

Prerequisites

Make sure that you have the required C•CURE system configuration settings.

- Server URL of the C•CURE system
- C•CURE Operator profile administrator user name and password to authenticate API access
- Client name to identify the Digital Badge service integrating with C•CURE
- Mapped custom values in the C•CURE system to Digital Badge service to set up access to doors and enable or deactivate both physical and digital badges.
  - **Employee email address database field name.** This is the custom field used to look up users by email address. For example, Text4.
  - **Smart ID.** Smart ID is used by the BLE (Bluetooth low energy) reader,
  - **CHUID.** Enter the cardholder unique identifier card format for CHUID. This is the system-generated cardholder unique ID sent to the panel.
  - **Facility Code.** Used to specify the facility code for user badges. The Standard Credential field is optional for Facility Code.
  - **Card Authentication Key (CAK) Issuer.**
  - **Product Authorization Key (PAK) Issuer.**

**Procedure**

1. Click **C•CURE Configuration** on the Digital Badge page and enter the C•CURE system configuration details.

2. In the form, enter the following.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Name</td>
<td>Default is Digital Badge. You do not need to change this unless there is a different internal naming convention preferred.</td>
</tr>
<tr>
<td>Server URL</td>
<td>If using a reverse proxy, enter the public URL. For example, <a href="https://digitalbadge-workspace.mycompany.com">https://digitalbadge-workspace.mycompany.com</a>. If no reverse proxy, enter the URL of the C•CURE system.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the operator profile administrator user name that can authenticate to the C•CURE service. This name follows the Windows domain/username format.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with the operator profile administrator user name.</td>
</tr>
<tr>
<td>Employee Email Address Database Field Name</td>
<td>Enter the custom field in C•CURE used to look up users by email address. For example, Text4.</td>
</tr>
<tr>
<td>Smart ID</td>
<td>Enter the desired identifier for the Smart ID used for the Bluetooth handshake, for instance AA.</td>
</tr>
<tr>
<td>CHUID</td>
<td>Enter the desired format for CHUID. For instance, 0.</td>
</tr>
<tr>
<td>Facility Code</td>
<td>Enter the desired identifier for Facility Code. For instance, 5878.</td>
</tr>
<tr>
<td>CAK issuer</td>
<td>Enter the desired value for CAK Issuer. If none is known, provide a default value of null.</td>
</tr>
<tr>
<td>PAK issuer</td>
<td>Enter the desired value for PAK Issuer. If none is known provide a default value of null.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Enter the client application’s license GUID in string format.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Enter the CCure integration’s version number. This number is defined as a value between 2.80 and 2.89. For example, 2.80</td>
</tr>
</tbody>
</table>

3. Enable **Hub Digital Badge.**
4 Click **Save**.

One version of the Digital Badge services can be configured in Hub Services and you can enable Digital Badge at the global level. You can also activate the Digital Badge service in templates. You can deactivate Digital Badge as a global feature and assign Digital Badge to specific templates. Assigning Digital Badge to templates, lets you manage the groups who can access the Digital Badge service. See [Chapter 5 Using Hub Templates to Customize the Workspace ONE Intelligent Hub Experience for Different Users](#).

**Managing the Digital Badge Experience for End Users (Cloud only)**

The following describes deployment considerations and recommendations to present the best experience for end users who use the Digital Badge service in the Workspace ONE Intelligent Hub app.

When you set up the Digital Badge service, targeted users receive a priority notification in the Workspace ONE Intelligent Hub app for iOS or Android devices to introduce the Digital Badge service and to ask them to activate Hub Digital Badge on their device.

When you activate Digital Badge in the Workspace ONE Intelligent Hub app, when a user goes near a HID door access reader, the Workspace ONE Intelligent Hub app indicates that it is in proximity and attempts to issue an unlock command. When successful, users see a green check indicator in the Workspace ONE Intelligent Hub app.

Users can deactivate Digital Badge in the Preferences section in the Workspace ONE Intelligent Hub app, accessed from their avatar image.
The Digital Badge service is enabled on one mobile device at a time. To change devices, users deactivate Digital Badge on the device that is currently enabled. Then they activate Digital Badge on the new device.

The following are recommendations for a good user experience with Digital Badge.

- Make sure that users enable the Allow Notifications setting for the Workspace ONE Intelligent Hub app on their devices. When Allow Notification is enabled, users receive a notification on their device every time the Workspace ONE Intelligent Hub app unlocks a door. If Allow Notification is not enabled, users can still unlock doors, but they do not receive notifications on their device as an indicator that a door has unlocked.

- Make sure that users enable the Location setting to Always on in iOS and Allow all the time on in Android for the Workspace ONE Intelligent Hub app on their devices. When the Location setting is enabled with those values, Workspace ONE Intelligent Hub app can unlock doors when the app is in the background or is closed. If Location is not set to those values, users must open the Workspace One Intelligent Hub app to open the door.

- Note that if Near Field Communication (NFC) is enabled in addition to Bluetooth, iOS devices automatically trigger the Wallet if the Wallet contains a credit card or passes. This does not prevent Workspace ONE Intelligent Hub app from unlocking a door, but Wallet temporarily covers the Intelligent Hub app.

- Configure the BLE reader to require that the user’s device be no more than a foot away from the door to open it. If the distance is set to far out, unintended doors might unlock.

Creating a Health Attestation Return-to-Work Notification in Hub Services (Cloud only)

The Digital Badge service can be used along with health attestation surveys to manage an employee’s temporary access to buildings based on survey answers. Employees complete a health screening questionnaire before they can enter a building and return to work.

To use health attestation survey results to manage access to buildings, the Hub Digital Badge service must be configured and integrated with Physical Access Control systems (PACS) Software House C•CURE 9000.

Admins use the Notification Builder in Hub Services to create custom return-to-work notifications that are used for health attestation screening. The health screening questions in the notification can be targeted to employees based on location and time zone. The location that employees select when they complete the survey determines the time zone and how many days the Intelligent Hub app can be used as a badge before access is deactivated.

You add the locations that can be selected to the Locations table in the Digital Badge service page. You give the locations a name that employees can recognize, select the time zone for each location, and specify the number of days that the badge is enabled. Valid access can be set between 1 and 90 days.
When a return-to-work notification is sent, the notification displays at the top of the For You page in the Workspace ONE Intelligent Hub app. Employees who are expected to return to work must complete the survey to confirm that they are not experiencing any of the symptoms outlined in the survey. When employees submit their answers, Hub Services analysis the answers. The employee receives a notification that they either passed or failed. If they passed the survey, the Digital Badge service enables Workspace ONE Intelligent Hub to act as a physical badge to access buildings. If the employee fails the survey, employees are informed about how to retake the survey. The ability to access the building is deactivated in the app.

**Use Notification Builder to Create the Notification**

You use the Notification Builder in Hub Services to create an actionable notification to ask employees to answer health questions so that they can return to work. Employees review the questions and select either Yes or No and submit their answers.

**Prerequisites**

- Your company’s locations configured in the Location list in the Digital Badge service.  
- To take the health screening survey and use the app as a badge, the Workspace ONE Intelligent Hub app on employee devices must be 20.10 or later.

**Procedure**

1. Navigate to the Hub Services Notifications page and click **Create Custom Notification**.
2. Enter the name to identify this notification as the health attestation survey.
3. Select the audience and the group that are to receive this notification.
4. Select **Return to Work** as the priority type.
5. Click **Next** to go to the Content page. In the Content page, complete the notification message details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Use the default image, Intelligent Hub or you can add your own image for this notification.</td>
</tr>
<tr>
<td>Title</td>
<td>Enter a title for the notification. This displays in the message header.</td>
</tr>
<tr>
<td>Location</td>
<td>The locations configured in the Digital Badge Location table are listed. Select the locations that apply to this survey. Employees select their location when they complete the survey.</td>
</tr>
<tr>
<td>Survey</td>
<td>Type the survey questions in the text box. The questions can require only a Yes or No answer. The health attestation analysis process in Hub Services is configured to reject the return to work request if any answers are Yes. When this happens, the Workspace ONE Intelligent Hub app revokes both the digital and physical badge access.</td>
</tr>
</tbody>
</table>
6 Click **Next** to go to the Scheduling page. Select the expiration date, hour, and time zone when the health attestation notification will expire, after which the notification can no longer be used to take the survey.

7 Click **Next** to review the notification.

8 Click **Create** to create and send the notification.

Users see the notification at the top of the For You page in the Workspace ONE Intelligent Hub app.

### Resend the Return-to-Work Notification

You can resend a return-to-work notification that you created. Before you resend it, you can extend the expiration date of the sticky notification. You cannot edit the message.

New users added to the target audience group and existing users see the resent return-to-work notification at the top of the For You page in the Workspace ONE Intelligent Hub app.

1 Navigate to the Hub Services Notifications page and select the Health Attestation Return-to-Work notification to resend.

   **Note** Only sticky notification types can be resent.

2 Click the **Resend Notification** button that displays above the Notification list.

3 Change the expiration date, if you want to extend how long the return-to-work notification can be accessed.

4 Click **NEXT** to review the summary and then click **SEND**.

### Employee Experience When They Receive a Health Attestation Notification in Workspace ONE Intelligent Hub App (Cloud only)

Employees who are required to complete the health screening attestation before they can return to work receive a priority return to work notification that displays at the top of the For You page in Workspace ONE Intelligent Hub app on their registered device.

When Digital Badge is activated, employees can receive the health attestation notification, complete the survey and automatically have their physical and digital badge activated or deactivated based on their answers.
The badge is enabled for return to work based on the number of days set up for that location in the Digital Badge Location pages.
About MDM Enrollment in Workspace ONE Intelligent Hub

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

To enroll devices using the Intelligent Hub app, you can ask your users to download the 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 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.

This chapter includes the following topics:

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

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 Intelligent Hub employee self-service tab on devices and in the web browser.

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 guide in the Platform Guides section in the Workspace ONE UEM Documentation center.

### Table 12-1. Workspace ONE Intelligent Hub Settings Descriptions

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Disable Unenroll Option in Intelligent Hub.</td>
<td>This setting allows or blocks the ability for a user to unenroll from the Intelligent Hub. When this box is selected, the unenroll option is deactivated. The setting label is changed to <strong>Reenroll</strong>, to allow the user to enroll the device to another user but not be able to remove the MDM profile.</td>
</tr>
<tr>
<td></td>
<td>Background App Refresh</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Minimum Refresh Interval</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Transmit on Wi-Fi only</td>
<td>This setting requires that any samples or communication must take place over Wi-Fi only and not a cellular network.</td>
</tr>
<tr>
<td>Area</td>
<td>Collect Location Data</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Detect iBeacon Area</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 12-1. Workspace ONE Intelligent Hub Settings Descriptions (continued)

<table>
<thead>
<tr>
<th>Section Name</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Collect Cellular Data Usage</td>
<td>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.</td>
</tr>
<tr>
<td>Self Service Setting</td>
<td>Self Service Enabled</td>
<td>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.</td>
</tr>
<tr>
<td>SDK Profile</td>
<td>SKD Profile (Legacy)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SDK Profile V2</td>
<td>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.</td>
</tr>
</tbody>
</table>

Enable Intelligent Hub Device Enrollment and Authentication Mode

You select the authentication mode and enable direct device enrollment for the 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 Intelligent Hub app without integrating with Workspace ONE Access. Select Workspace ONE Access when the 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 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.
Enable Unmanaged Enrollment for iOS Devices

Devices enrolled through the 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 the 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](https://docs.vmware.com) page.

Configure Email and Phone Number Contact Information for 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 Intelligent Hub app Support tab.
When you configure device enrollment settings in 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 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.

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.
<table>
<thead>
<tr>
<th>Access Type</th>
<th>Features</th>
<th>Description</th>
<th>Suggested Uses</th>
</tr>
</thead>
</table>
| Open Access (unmanaged) | - 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. | Users access resources on their device without granting admins permission to access their device. 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. | - 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 | - 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. | Users install a management profile on their device to grant admins permission to access their device. Applications with managed access are available to devices that Workspace ONE UEM manages. 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. | - 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

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 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 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

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 Workspace ONE UEM-managed Android devices. With mobile SSO, users to 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**.
4 In the Android EMM Registration section, click **Configure**.

5 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.

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

7 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.

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

Results

You are now ready to enroll Android devices using Android Enterprise.
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 smartphone, tablet, or desktop computer.

This chapter includes the following topics:

- 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 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 VMware Workspace ONE 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 Intelligent Hub users in the following tab settings.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>Enter and view information concerning supported device models, ratings, and categories.</td>
</tr>
<tr>
<td>Assignment</td>
<td>Assign the Workspace ONE Intelligent Hub apps to smart groups of end users who can use the application on their device.</td>
</tr>
<tr>
<td>Deployment</td>
<td>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.</td>
</tr>
<tr>
<td>Terms of Use</td>
<td>(Optional) Enable Terms of Use for using the Workspace ONE Intelligent Hub application.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Platform</th>
<th>Configuration Key</th>
<th>Value Type</th>
<th>Configuration Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>AppServiceHost</td>
<td>String</td>
<td><code>&lt;VMware Workspace ONE UEM Server URL&gt;</code></td>
<td>Configures the server URL for VMware Workspace ONE Intelligent Hub on devices.</td>
</tr>
<tr>
<td>iOS</td>
<td>deviceUDID</td>
<td>String</td>
<td><code>{DeviceUid}</code></td>
<td>Tracks the devices used to authenticate to the Workspace ONE Access environment.</td>
</tr>
<tr>
<td>iOS</td>
<td>SkipDiscoveryScreen</td>
<td>Boolean</td>
<td><code>true</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 13-1. Intelligent Hub Managed Device Configurations Options in Workspace ONE UEM Console (continued)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Configuration Key</th>
<th>Value Type</th>
<th>Configuration Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android and iOS</td>
<td>RemoveAccountSignOut</td>
<td>Integer</td>
<td>0 - The Remove Account option displays</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - The Remove Account option does not display</td>
<td>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.</td>
</tr>
</tbody>
</table>

Deploying Workspace ONE Intelligent Hub App for macOS

The 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 Intelligent Hub app.

You can configure settings to automatically install the 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 Intelligent Hub 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 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, Microsoft Edge, and Internet Explorer 11.

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

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, tables, 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.

This chapter includes the following topics:

- 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 Apps 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.

In the Workspace ONE Intelligent Hub view from a browser, the navigation tabs are at top of the page. If you enabled Favorites, the Favorites tab displays before the Apps tab.
Figure 14-2. Workspace ONE Intelligent Hub Web Portal View

Workspace ONE Intelligent Hub App Account Settings

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

- **Notifications.** Users can manage Hub notifications, including receiving notifications sent from the mobile flows service.
- **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 or portal whenever they want.

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.

Receiving Notifications in the Workspace ONE Intelligent Hub App

When the Notifications feature is enabled 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 for information that is critical for the user to review and respond to on a timely basis as either high-priority or urgent. 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 14-1. Types of Notifications Received in Workspace ONE Intelligent Hub App

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Notifications</td>
<td>As an admin, you can create custom notifications.</td>
</tr>
<tr>
<td>![Custom Notification Image]</td>
<td></td>
</tr>
<tr>
<td>Approval Request through Workspace ONE mobile flows</td>
<td>Users can approve or deny approval notifications.</td>
</tr>
<tr>
<td>![Approval Request Image]</td>
<td></td>
</tr>
<tr>
<td>New App Availability</td>
<td>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.</td>
</tr>
<tr>
<td>![New App Availability Image]</td>
<td></td>
</tr>
</tbody>
</table>

When users click an action button to respond to the notification, the notification is moved to the History folder. The notification is archived in History 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 Accounts page, they can also manage notification for any other business systems apps that generate notifications through mobile flow.

**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 Apps in a Web Browser**

The web browser catalog page layout you configured in Hub Services displays in Workspace ONE Intelligent Hub when users open Hub catalog in a browser.

New apps display in the new apps section. Users can access their apps, install apps, including virtual apps that they are entitled to. When apps are organized into logical categories, these categories are displayed.

**Note** Mobile applications are not available from the Hub portal view in a browsers.
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 the Change Password option is configured, they can click **Change Password** to change their password.

In the Account Settings Preferences section, users set their preference for 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.

In the Account Settings Notifications Integrations section, users can deactivate specific types of mobile flows notifications. Changing this notification setting affects notifications on all devices.
Frequently Asked Questions about the VMware Workspace ONE Intelligent Hub

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 inactivity.

- 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 Digital Badge?**

Digital Badge enables you to use Workspace ONE Intelligent Hub on your mobile device to open doors of buildings on your campus. Currently this requires support from the badge-reader company as well your administrator.

This feature 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

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, Android Mobile Single Sign-On to VMware Workspace ONE
  - 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
  - Configuring AirWatch Provisioning app in Workspace ONE Access