

Workspace ONE System Settings Reference Manual for On-Premises Customers

VMware Workspace ONE UEM 1811



vmware®

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

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

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1 Overview 8

[System Settings for the Workspace ONE UEM console](#) 8

2 System 10

[System / Getting Started](#) 11

[System / Branding](#) 12

[System / Enterprise Integration / Enterprise Integration Services](#) 13

[System / Enterprise Integration / Certificate Authorities](#) 13

[System / Enterprise Integration / VMware Enterprise Systems Connector](#) 13

[System / Enterprise Integration / Directory Services](#) 14

[System / Enterprise Integration / Email \(SMTP\)](#) 20

[System / Enterprise Integration / VMware Tunnel / Configuration](#) 21

[System / Enterprise Integration / Tunnel / Network Traffic Rules](#) 21

[System / Enterprise Integration / Third Party Proxies](#) 21

[System / Enterprise Integration / Peer Distribution / Peer Distribution Software Setup](#) 22

[System / Enterprise Integration / CDN / Akamai](#) 22

[System / Enterprise Integration / Pull Service Installers](#) 22

[System / Enterprise Integration / SMS](#) 22

[System / Enterprise Integration / Syslog](#) 23

[System / Enterprise Integration / Remote Management](#) 24

[System / Enterprise Integration / VMware Identity Manager](#) 24

[System / Enterprise Integration / VMware Identity Manager/ Configuration](#) 25

[System / Enterprise Integration / VMware Identity Manager/ Access Management](#) 25

[System / Security / Restricted Actions](#) 26

[System / Security / Data Security](#) 29

[System / Security / SSL Pinning](#) 29

[System / Security / SSL Pinning / Requirements](#) 30

[System / Security / SSL Pinning / Configure](#) 30

[Upload SSL Device Services Certificate](#) 32

[System / Security / Trust Service](#) 33

[System / Security / Key Management](#) 33

[System / Help](#) 34

[System / Localization / Language Activation](#) 34

[System / Localization / Localization Editor](#) 35

[System / Report Subscriptions](#) 35

[System / Terms of Use](#) 36

[System / S/MIME](#) 36

[System / Advanced / Hub URLs](#) 37

System / Advanced / API / Event Notifications	37
System / Advanced / API / REST API	39
System / Advanced / API / SOAP API	40
System / Advanced / Device Root Certificate	41
System / Advanced / Secure Channel Certificate	41
System / Advanced / Service URLs	42
System / Advanced / Site URLs	42
System / Advanced / Query String Authentication	43
System / Advanced / Other	43

3 Devices & Users 45

Devices & Users / General / Enrollment	47
Devices & Users / General / Friendly Name	54
Devices & Users / General / Lookup Fields	55
Devices & Users / General / Message Templates	55
Devices & Users / General / Notifications	56
Devices & Users / General / Privacy	57
Devices & Users / General / Shared Device	58
Devices & Users / General / Advanced	60
Devices & Users / Android / Android EMM Registration	61
Devices & Users / Android / Hub Settings	62
Devices & Users / Android / Google Play Integration	67
Devices & Users / Android / Auto-Enrollment	67
Devices & Users / Android / Service Applications	68
Devices & Users / Android / Security	69
Devices & Users / Android / Samsung Enterprise FOTA	70
Devices & Users / Apple / APNs for MDM	70
Devices & Users / Apple / Apple iOS / APNs for Applications	70
Devices & Users / Apple / Apple iOS / Hub Settings	70
Devices & Users / Apple / Apple iOS / Managed Settings	72
Devices & Users / Apple / Apple macOS / Hub Application	73
Devices & Users / Apple / Apple macOS / Hub Settings	74
Devices & Users / Apple / Apple macOS / Software Management	75
Devices & Users / Apple / AppleCare	76
Devices & Users / Apple / Automated Enrollment	76
Devices & Users / Apple / MDM Sample Schedule	77
Devices & Users / Apple / Device Enrollment Program	78
Devices & Users / Apple / Profiles	78
Devices & Users / Apple / SCEP	79
Devices & Users / Apple / Install Fonts	79
Devices & Users / Apple / Education	80

Devices & Users / Blackberry / Blackberry 10 / General	80
Devices & Users / Blackberry / Blackberry 10 / Hub Settings	81
Devices & Users / Blackberry / Blackberry 10 / BES 10 Settings	81
Devices & Users / Blackberry / Legacy Blackberry / Hub Settings	82
Devices & Users / BlackBerry / Legacy BlackBerry / BES Settings	83
Devices & Users / QNX / Hub Settings	84
Devices & Users / Tizen / Hub Settings	86
Devices & Users / Chrome OS / Hub Settings	86
Devices & Users / Windows / Windows Auto-Discovery	87
Devices & Users / Windows / Windows Rugged / Hub Application	87
Devices & Users / Windows / Windows Rugged / Hub Settings	88
Devices & Users / Windows / Windows Rugged / Power on Password	91
Devices & Users / Windows / Windows Rugged / Metrics	91
Devices & Users / Windows / Windows Rugged / Advanced	92
Devices & Users / Windows / Windows Phone / Intelligent Hub Application	92
Devices & Users / Windows / Windows Phone / Hub Settings	93
Devices & Users / Windows / Windows Phone / Company Hub Settings	94
Devices & Users / Windows / Windows Phone / MDM Sample Schedule	95
Devices & Users / Windows / Windows Phone / Windows Health Attestation	95
Devices & Users / Windows / Windows 7 / Hub Application	97
Devices & Users / Windows / Windows 7 / Hub Settings	97
Devices & Users / Windows / Windows Desktop / General	99
Devices & Users / Windows / Windows Desktop / Hub Application	99
Devices & Users / Windows / Windows Desktop / Hub Settings	100
Devices & Users / Windows / Windows Desktop / App Deployments	101
Devices & Users / Windows / Windows Desktop / Enterprise Apps	102
Devices & Users / Windows / Windows Desktop / Windows Sample Schedule	102
Devices & Users / Windows / Windows Desktop / Windows Health Attestation	103
Devices & Users / Peripherals / Server	104
Devices & Users / Peripherals / Sample Schedule	104
Devices & Users / Advanced / Bulk Management	105
Devices & Users / Advanced / Custom Fields	106
Devices & Users / Advanced / Device Groups	106
Devices & Users / Advanced / Area	106
Devices & Users / Advanced / Tags	107
Devices & Users / Advanced / User Categories	107
Devices & Users / Advanced / User Migration	107
Devices & Users / Advanced / Unmanaged Device Wipe Protection	108
Devices & Users / Advanced / Managed Device Wipe Protection	109
Devices & Users / Advanced / Profile Options	109

4 Apps 110

- [Apps / App Scan / Third-Party Integration 111](#)
- [Apps / Application Integration / TouchDown 113](#)
- [Apps / Browser 113](#)
- [Apps / Workspace ONE / Catalog / General 116](#)
- [Apps / Workspace ONE / Catalog / Standalone Catalog 117](#)
- [Apps / Workspace ONE / App Restrictions 118](#)
- [Apps / Workspace ONE / Application Categories 118](#)
- [Apps / Workspace ONE / External App Repository 119](#)
- [Apps / Workspace ONE / Application Removal Protection 119](#)
- [Apps / Workspace ONE / Catalog / Featured Applications 120](#)
- [Devices & Users / Apple / VPP Managed Distribution 120](#)
- [Apps / Workspace ONE / Paid Public Applications 121](#)
- [Apps / Container 122](#)
- [Apps / Inbox 122](#)
- [Apps / Video 123](#)
- [Apps / Settings and Policies / Security Policies 124](#)
- [Apps / Settings and Policies / Settings 124](#)
- [Apps / Settings and Policies / Profiles 124](#)
- [Apps / Microsoft Intune® App Protection Policies 124](#)

5 Content 125

- [Content / Applications / Content Locker Sync 126](#)
- [Content / Applications / Workspace ONE Content App 126](#)
- [Content / Content Gateway 128](#)
- [Content / Personal Content 129](#)
- [Content / User Storage 131](#)
- [Content / Remote Storage 132](#)
- [Content / Content Viewer 132](#)
- [Content / Advanced / File Extensions 133](#)
- [Content / Advanced / Onboarding 134](#)

6 Email 135

- [Email / Configuration 135](#)
- [Email / Email Notification 135](#)

7 Telecom 137

- [Telecom / General 137](#)
- [Telecom / Jasper Integration 138](#)

8 Admin 139

Admin / Console Security / General	140
Admin / Console Security / Passwords	141
Admin / Console Security / Session Management	142
Admin / Data Purging	142
Admin / Cloud Services	142
Admin / Diagnostics / Logging	143
Admin / Diagnostics / System Health	144
Admin / Events	144
Admin / Licenses / Device	144
Admin / Monitoring	145
Admin / Scheduler	145
Admin / Settings Management / Settings Audit	148
Admin / Settings Management / Settings Summary	148
Admin / Settings Management / Settings Comparison	148
Admin / Storage	148
Admin / Troubleshooting / Web Console Log	149
Admin / Troubleshooting / Directory Connectivity Tool	149
Admin / Troubleshooting / SCEP Certificate Tool	149
Admin / Content Delivery Settings	149
Admin / Policy Engine Settings	150
Admin / Data Samples	150
Admin / Custom Attribute Settings	151
Admin / Product Provisioning	151
Admin / Product Improvement Programs	151

9 Installation 153

Installation / Memcached Settings	153
Installation / File Path	154
Installation / Installation Checklist	154
Installation / Maps	154
Installation / Performance Tuning	155
Installation / Proxy	157
Installation / Reports	158
Installation / Advanced / Endpoints	159
Installation / Advanced / File Sync	159
Installation / Advanced / Other	159

Overview

1

This chapter includes the following topics:

- [System Settings for the Workspace ONE UEM console](#)

System Settings for the Workspace ONE UEM console

The settings page enables you to configure all the "behind the scenes" settings that dictate how Workspace ONE UEM powered by AirWatch operates.

Where applicable, you can find references to additional documentation. Some systems settings pages contain mostly legacy settings that are typically not configured or used. These settings are pointed out with a recommendation not to alter them unless instructed to do so by Workspace ONE UEM.

Settings are split across eight sections, depending upon your deployment and permissions.

- [Chapter 2 System](#)
- [Chapter 3 Devices & Users](#)
- [Chapter 4 Apps](#)
- [Chapter 5 Content](#)
- [Chapter 6 Email](#)
- [Chapter 8 Admin](#)
- [Chapter 9 Installation](#)

SaaS vs. On-Premises

This help contains all of the system settings available for the highest level of access. This may not apply to your administrator role or deployment type.

There are two versions of this guide – one for SaaS and one for on premises. Ensure you are viewing the correct document that pertains to your Workspace ONE UEM deployment. You are currently reading the on-premises version of the guide. Access these documents on docs.vmware.com.

Note the following distinction between on-premises and SaaS deployments:

- **On-premises** refers to Workspace ONE UEM deployments where your organization hosts all Workspace ONE UEM components and servers on its internal networks. Administrators for on-premises deployments can see additional system settings, and System Administrators can see more still.
- **SaaS** refers to Workspace ONE UEM deployments where certain components, such as the Console and API servers, are hosted in the cloud. UEM console Administrators will be able to see the system settings that correlate to the SKUs their organization has purchased.

SKUs and Available Settings

While this section covers all of the available Workspace ONE UEM settings, you may or may not see certain sections depending on the SKUs you have purchased. If you do not see a particular section or settings page in your Workspace ONE UEM console then you need to first purchase the SKU for that feature. Please see the Workspace ONE UEM Pricing page (<http://www.air-watch.com/pricing/>) for additional information.

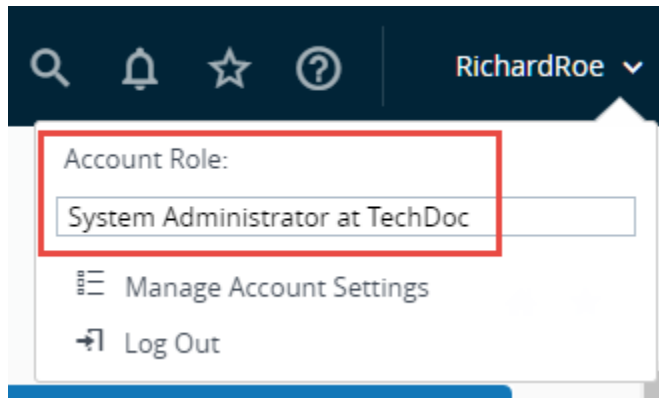
Settings at the Global Level for On-Premises Customers

Certain settings may only be configured at the Global organization group. We have attempted to document this requirement for each applicable settings page, but if you cannot see a particular page or particular settings on the page, then configuring at Global may be a requirement. In general, the settings page should indicate when this is a requirement.

Admin and Installation Settings for On-Premises Customers

The Admin and Installation settings within the Workspace ONE UEM console system settings will differ depending on your administrator role. In general, **Administrator roles** have access to most Admin / Installation settings, while **System Administrator roles** have access to all of them. If there are certain settings you do not see but want to access, please contact your System Administrator, which should have access to these settings.

You can check what your role is by selecting the Account icon.



System

2

Provides information about Workspace ONE UEM System settings.

The System settings are categorized into the following:

This chapter includes the following topics:

- [System / Getting Started](#)
- [System / Branding](#)
- [System / Enterprise Integration / Enterprise Integration Services](#)
- [System / Enterprise Integration / Certificate Authorities](#)
- [System / Enterprise Integration / VMware Enterprise Systems Connector](#)
- [System / Enterprise Integration / Directory Services](#)
- [System / Enterprise Integration / Email \(SMTP\)](#)
- [System / Enterprise Integration / VMware Tunnel / Configuration](#)
- [System / Enterprise Integration / Tunnel / Network Traffic Rules](#)
- [System / Enterprise Integration / Third Party Proxies](#)
- [System / Enterprise Integration / Peer Distribution / Peer Distribution Software Setup](#)
- [System / Enterprise Integration / CDN / Akamai](#)
- [System / Enterprise Integration / Pull Service Installers](#)
- [System / Enterprise Integration / SMS](#)
- [System / Enterprise Integration / Syslog](#)
- [System / Enterprise Integration / Remote Management](#)
- [System / Enterprise Integration / VMware Identity Manager](#)
- [System / Security / Restricted Actions](#)
- [System / Security / Data Security](#)
- [System / Security / SSL Pinning](#)
- [System / Security / SSL Pinning / Requirements](#)

- [System / Security / SSL Pinning / Configure](#)
- [Upload SSL Device Services Certificate](#)
- [System / Security / Trust Service](#)
- [System / Security / Key Management](#)
- [System / Help](#)
- [System / Localization / Language Activation](#)
- [System / Localization / Localization Editor](#)
- [System / Report Subscriptions](#)
- [System / Terms of Use](#)
- [System / S/MIME](#)
- [System / Advanced / Hub URLs](#)
- [System / Advanced / API / Event Notifications](#)
- [System / Advanced / API / REST API](#)
- [System / Advanced / API / SOAP API](#)
- [System / Advanced / Device Root Certificate](#)
- [System / Advanced / Secure Channel Certificate](#)
- [System / Advanced / Service URLs](#)
- [System / Advanced / Site URLs](#)
- [System / Advanced / Query String Authentication](#)
- [System / Advanced / Other](#)

System / Getting Started

The Getting Started settings page lets you configure settings related to the Getting Started feature of the Workspace ONE UEM console.

Note This setting is only configurable at a Customer-level organization group.

Setting	Description
Getting Started Workspace ONE Status	Select to Enable or Disable (skip) the Workspace ONE section of the Getting Started wizard.
Getting Started Device Status	Select to Enable or Disable (skip) the Mobile Device Management section of the Getting Started wizard.

Setting	Description
Getting Started Content Status	Select to Enable or Disable (skip) the Mobile Content Management section of the Getting Started wizard.
Getting Started Application Status	Select to Enable or Disable (skip) the Mobile Application Management section of the Getting Started wizard.

You can resume or skip any of these sections at any time by navigating to **Getting Started** in the navigation pane of the UEM console.

System / Branding

The Branding settings page lets you configure settings related to the branding of the Workspace ONE UEM console. Change branding to reflect company colors or visually delineate specific organization groups.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Branding Tab

Setting	Description
Company Logo	The logo that appears in the top-left of the console, the login splash page, and About Workspace ONE UEM popup. The maximum resolution of the image is 800x300.
Login Page Background	The image that displays on the login page. The suggested resolution of the image is 1024x768.
Self-Service Portal Login Page Background	The image that displays on the self-service portal login splash page. The suggested resolution of the image is 1024x768.
Company Website URL	Selecting the company logo on the Workspace ONE UEM site leads to this URL. If this setting is left blank, selecting the company logo leads to the admin home page.

Colors

Here you can set the color schemes for the UEM console, with a mockup illustrating your changes.

Custom CSS Tab

Setting	Description
Custom CSS	Insert a cascading style sheet of your own custom design that will override the console defaults.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Enterprise Integration / Enterprise Integration Services

The Enterprise Integration Services settings page is used to configure the EIS component. Note that EIS has been upgraded into the VMware Enterprise Systems Connector and VMware Tunnel components. You will therefore not enable or configure EIS using this page if you are using either of those components. You may see a button to **Transfer Settings**, which lets you migrate your current EIS settings.

System / Enterprise Integration / Certificate Authorities

The Certificate Authorities (CA) settings page is used to configure integration with various certificate authorities. Rather than configure specific settings, it is here that you actually add a CA and create its request template. Available actions are listed below.

Certificate Authorities Tab

- Select the **Add** button to add a new CA.
- Select the **Edit** (pencil) icon for an existing CA to edit it.
- Select the radio button for an existing CA and then select the **Delete** (X) icon to delete the CA.

Request Templates Tab

- Select the **Add** button to add a new request template.
- **Certificate Authority** – Select a CA from the drop-down list to view the request templates associated to it.
- Select the **Edit** (pencil) icon for an existing request template to edit it.
- Select the radio button for an existing request template and then select the **Delete** (X) icon to delete the request template.

System / Enterprise Integration / VMware Enterprise Systems Connector

The VMware Enterprise Systems Connector settings page is used to configure the VMware Enterprise Systems Connector component. Note that if you already have EIS configured then you will need to disable it by unchecking its check box on the EIS settings page. You may see a button to **Transfer Settings**, which lets you migrate your current EIS settings.

For information on VMware Enterprise Systems Connector setup, configuration, and installation – including information about the system settings, search for **AirWatch Cloud Connector** in docs.vmware.com.

System / Enterprise Integration / Directory Services

The directory services settings page lets you configure your directory service integration with Workspace ONE UEM. In addition to manually configuring the settings below, you can also select **START SETUP WIZARD** from the bottom of the page.

Note Before you are able to make changes to the Directory Services settings, you must ensure that the **Directory** check box is enabled (checked) in the **Authentication Mode(s)** option found in the **Device & Users > General > Enrollment** page. See [Devices & Users / General / Enrollment](#). Override the **Current Setting** for the above-linked page if necessary.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Server Tab

Setting	Description
LDAP	
Directory Type	Select the type of directory service that your organization uses. Workspace ONE UEM supports open source LDAP for directory services.
DNS SRV	Allow the Domain Name System Service Record to decide which server in its prioritized list of servers can best support LDAP requests. This feature ensures continuity of services in a high availability environment. The default setting is Disabled. With this option disabled, Workspace ONE UEM uses your existing directory server, the address of which you enter in the Server setting. Supported DNS servers: <ul style="list-style-type: none"> ■ Active Directory integrated Microsoft DNS servers ■ Standalone Microsoft DNS servers
Server	Enter the address of your directory server. This setting is only available when Enable DNS SRV is Disabled.
Encryption Type	Select the type of encryption to use for a directory services communication. The options available are None (unencrypted), SSL , and Start TLS .
Port	Enter the Transmission Control Protocol (TCP) port used to communicate with the domain controller. The default for unencrypted LDAP directory service communication is port 389. To view a KnowledgeBase article that lists the most up-to-date Workspace ONE UEM SaaS data center IP ranges, refer to https://support.air-watch.com/articles/115001662168 . <ul style="list-style-type: none"> ■ When you change the Encryption Type setting to SSL, the Port setting automatically changes to 636. ■ When you select the Add Domain button, the Port setting automatically changes to 3268.
Verify SSL Certificate	This setting is only available when the Encryption Type is SSL or Start TLS . Receive SSL errors by selecting the SSL check box.
Protocol Version	Select the version of the Lightweight Directory Access Protocol (LDAP) that is in use. Active Directory uses LDAP versions 2 or 3. If you are unsure of which Protocol Version to use, try the commonly used value of '3'.

Setting	Description
Use Service Account Credentials	Use the App pool credentials from the server on which the VMware Enterprise Systems Connector is installed for authenticating with the domain controller. Enabling this option hides the Bind user name and Bind Password settings.
Bind Authentication Type	Select the type of bind authentication to enable the AirWatch server to communicate with the domain controller. You can select Anonymous , Basic , Digest , Kerberos , NTLM , or GSS-NEGOTIATE . If you are unsure of which Bind Authentication Type to use,. If unsure start by setting the bind authentication type to Basic . You will know if your selection is not correct when you click Test Connection .
Bind User Name	Enter the credentials used to authenticate with the domain controller. This account (which the entered user name identifies) allows a read-access permission on your directory server and binds the connection when authenticating users. If you are unsure of which Bind Authentication Type to use, try the commonly used GSS-NEGOTIATE. You will know if your selection is not correct when you click Test Connection.
Clear Bind Password	Select the Clear Bind Password check box to clear the bind password from the database.
Bind Password	Enter the password for the bind user name to authenticate with the directory server.
Domain /Server	Enter the default domain and server name for any directory-based user accounts. If only one domain is used for all directory user accounts, fill in the text box with the domain. This entry means that users are authenticated without explicitly stating their domain. You can add more domains by selecting the Add Domain option. Make sure that all the domains are in the same forest. In this case, Workspace ONE UEM automatically changes the port setting to 3268 for global catalog. You may choose to change the port setting to 3269 for SSL encrypted traffic, or override it completely by entering a separate port.
Is there a trust relationship between all domains?	This setting is available only when you have more than one domain added. Select Yes if the binding account has permission to access other domains you have added. This added permission means that the binding account can successfully log in from more domains.

The following options are available after selecting the **Advanced** section drop-down.

Setting	Description
Advanced	
Search Subdomains	Enable subdomain searching to find nested users. Leaving this option disabled can make searches faster and avoids network issues. However, users and groups located in subdomains under the base Domain Name (DN) are not identified.
Connection Timeout	Enter the LDAP connection timeout value (in seconds).
Request Timeout	Enter the LDAP query request timeout value (in seconds).
Search without base DN	Enable this option when using a global catalog and when you do not want to require a base DN to search for users and groups.
Use Recursive OID at Enrollment	Verify user group membership at the time of enrollment. As the system runs this feature at enrollment time, your performance may decrease with some directories.
Use Recursive OID For Group Sync	Verify user group membership at the time of Group synchronization.

Setting	Description
Object Identifier Data Type	Select the unique identifier that never changes for a user or group. The options available are Binary and String . Typically, the Object Identifier is in a Binary format.
Sort Control	Option to enable sorting. If this option is disabled, it can make searches faster and you can avoid sync timeouts.

Azure Active Directory

Select **Enabled** for **Use Azure AD for Identity Services** and follow the on-screen steps to setup integration with Azure Active Directory. For more information, search for the topic **Enrollment Through Azure AD Integration** in docs.vmware.com.

SAML 2.0

The following Security Assertion Markup Language (SAML) options are available after selecting **Use SAML for Authentication**, and are only applicable if you are integrating with a SAML identity provider.

Setting	Description
Enable SAML authentication For	You have the choice of using SAML authentication for Admin , Enrollment , or Self Service Portal . UEM console administrators can select all three, or any combination of two, or select any one of the three components.
Use new SAML Authentication endpoint	<p>A new SAML authentication endpoint has been created for end-user authentication (device enrollment and login to SSP). This authentication replaces the two dedicated enrollment and SSP endpoints with a single endpoint.</p> <p>While you may choose to keep your existing settings, Workspace ONE UEM suggests updating your SAML settings to take advantage of the new combined endpoint.</p> <p>If you want to use the new endpoint, enable this setting and save the page. Then use the Export Service Provider Settings to export the new metadata file and upload it to your IdP. Doing so establishes trust between the new endpoint and your IdP.</p>

SAML 2.0

Import Identity Provider Settings	Upload a metadata file obtained from the identity provider. This file must be in Extensible Markup Language (XML) format.
Service Provider (Workspace ONE UEM) ID	Enter the Uniform Resource Identifier (URI) with which Workspace ONE UEM identifies itself to the identity provider. This string must match the ID that has been established as trusted by the identity provider.
Identity Provider ID	Enter the URI that the identity provider uses to identify itself. Workspace ONE UEM checks authentication responses to verify that the identity matches the ID provided here.

REQUEST

Request Binding Type	Select the binding types of the request. The options include Redirect , POST , and Artifact .
Identify Provider Single Sign On URL	Enter the identity provider's Uniform Resource Locator (URL) that Workspace ONE UEM uses to send requests.
NameID Format	Enter the format in which the identity provider sends a NameID for an authenticated user. This value is not required as Workspace ONE UEM obtains the user name from the FriendlyName "uid" required attribute.

Setting	Description
Authentication Request Security	Select from the dropdown whether or not the Service Provider (Workspace ONE UEM) signs the authentication requests. You can select None , Sign Authentication Requests (SHA1) , and Sign Authentication Requests (SHA256) . Consider selecting Sign Authentication Requests (SHA256) for a more secure authentication.
RESPONSE	
Response Binding Type	Select the binding types of the response. The options include Redirect , POST , and Artifact .
Sp Assertion URL	Enter the Workspace ONE UEM URL that the identity provider configures to direct its authentication responses. "Assertions" regarding the authenticated user are included in success responses from the identity provider.
Authentication Response Security	This value specifies whether the IdP signs the response. You can select between None , Validate Response Signatures , and Validate Assertions Signatures . Consider selecting Validate Response Signatures for a more secure authentication.
CERTIFICATE	
Identity Provider Certificate	Upload the identity provider certificate.
Service Provider (AirWatch) Certificate	Upload the service provider certificate.
Export Service Provider Settings button	Exports the metadata file for uploading to your Identity Provider (IdP). This setting establishes trust between the new SAML endpoint (for enrollment and SSP login) and your IdP.

What UEM Requires of Third-Party Identity Providers (IDP)

The following is universal for any Identity Provider (IDP).

■ All supported versions

- The third party IDP is required to send the following SAML attributes to Workspace ONE UEM:

SAML Attribute Name	SAML Attribute Format	SAML Attribute value
NameID	unspecified	TransientID
uid or sAMAccountName	unspecified	Username attribute from UEM

- To retrieve the **Username** attribute used by Workspace ONE UEM, take the following steps.
 - 1 Navigate to **System > Enterprise Integration > Directory Services**.
 - 2 Select the **Users** tab, then **Advanced** and look for the attribute named **Username**.
 - 3 The **Mapping Value** is the attribute required by Workspace ONE UEM. This could be **uid** or **sAMAccountName**, depending on the IDP.

■ Addendum for version 1904 and later (based on KB: <https://kb.vmware.com/s/article/2961194>)

- Replace the above table with the following table.

SAML Attribute Name	SAML Attribute Format	SAML Attribute Value
NameID	unspecified	TransientID

uid or sAMAccountName	unspecified	Username attribute from UEM
objectGUID	unspecified	Object Identifier attribute from UEM

User Tab

Setting	Description
User Object Class	Enter the appropriate Object Class. In most cases, this value is "user."
User Search Filter	<p>Enter the search parameter used to associate user accounts with Active Directory accounts. The suggested format is "<LDAPUserIdentifier>={EnrollmentUser}" where <LDAPUserIdentifier> is the parameter used on the directory services server to identify the specific user.</p> <ul style="list-style-type: none"> ■ For AD servers, use <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;">(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))</div> ■ For other LDAP servers, use <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;">(&(objectClass=inetOrgPerson)(uid={EnrollmentUser}))</div> <p>This format, (&(...)), must be used even when only a single search parameter is specified in either AD servers or other LDAP servers.</p> <ul style="list-style-type: none"> ■ For example, <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;">(&(uid={EnrollmentUser}))</div>

Advanced

Setting	Description
Auto Merge	Enable setting to allow user group updates from your directory service to merge with the associated users and groups in Workspace ONE UEM automatically.
Automatically Set Disabled Users to Inactive	<p>Select Enable to deactivate the associated user in Workspace ONE UEM when that user is disabled in your LDAP directory service (for example, Novell e-Directory).</p> <ul style="list-style-type: none"> ■ Value For Disabled Status – Enter a numeric value and select the type of Lightweight Directory Access Protocol (LDAP) attribute used to represent a user's status. Select "Flag Bit Match" if the user status is designated by a bitwise flag (which is the default for Active Directory). <p>When "Flag Bit Match" is selected, if any bits from the property match the entered numeric value, then directory service considers the user to be disabled. This setting is only visible when the option Automatically Set Disabled Users to Inactive is checked.</p> <p>Note If you select this option, then Workspace ONE UEM administrators set as inactive in your directory service are not able to log in to the Workspace ONE UEM console. In addition, enrolled devices assigned to users who are set as inactive in your directory service are automatically unenrolled.</p>
Enable Custom Attributes	Enable custom attributes. Custom Attributes is a section that appears under the main Attribute – Mapping Value table. You must scroll down to the bottom of the page to see the Custom Attributes.

Setting	Description
Attributes	<p>Review and edit the Mapping Values for the listed Attributes, if necessary. These columns show the mapping between Workspace ONE UEM user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in Active Directory (AD). Update these mapping values to reflect the values used for your own or other directory service types.</p> <p>If you add or remove a custom attribute, you should initiate a manual sync afterward by selecting the Sync Attributes button.</p>
Sync Attributes button	Manually sync the attributes mapped here to the user records in Workspace ONE UEM. Attributes sync automatically on the time schedule configured for the Workspace ONE UEM environment.

Group Tab

Setting	Description
Group Object Class	Enter the appropriate Object Class. In most cases this value should be group .
Organizational Unit Object Class	Enter the appropriate Organizational User Object Class.

Show Advanced

Setting	Description
Group Search Filter	Enter the search parameter used to associate user groups with directory service accounts.
Auto Sync Default	Select this checkbox to automatically add or remove users in Workspace ONE UEM configured user groups based on their membership in your directory service.
Auto Merge Default	Select this check box to automatically apply sync changes without administrative approval.
Maximum Allowable Changes	<p>Enter the number of maximum allowable group membership changes to be merged into Workspace ONE UEM. Any number of changes detected upon syncing with the directory service database under this number are automatically merged.</p> <p>If the number of changes exceed this threshold, an administrator must manually approve the changes before they are applied. A single change is defined by a user either leaving or joining a group. A setting of 100 Maximum Allowable Changes means the Console does not need to sync with your directory service as much.</p>
Conditional Group Sync	Enable this option to sync group attributes only after changes occur in Active Directory. Disable this option to sync group attributes regularly, regardless of changes in Active Directory.
Auto-Update Friendly Name	<p>When enabled, the friendly name is updated with group name changes made in active directory.</p> <p>When disabled, the friendly name can be customized so admins can tell the difference between user groups with identical common names. This can be useful if your implementation includes organizational unit (OU)-based user groups with the same common name.</p>
Attribute	Review and edit the Mapping Value for the listed Attribute , if necessary. These columns show the mapping between Workspace ONE UEM user attributes (left) and your directory service attributes (right). By default these attributes are values most commonly used in AD. Update these mapping values to reflect the values used for your own or other directory service types.

- **Test Connection** – Click this button to test your connection with your directory service endpoint.
- **Start Setup Wizard** – Click this button to launch the directory service setup wizard, which walks you through configuring DS integration.

Limitations and Caveats

- No AD passwords are stored in the Workspace ONE UEM database with the exception of the Bind account password used to link directory services into your Workspace ONE UEM environment. That password is stored in encrypted form in the database and is not accessible from the console. Unique session keys are used for each sync connection to the Active Directory server.
- In some instances global catalogs are used to manage multiple domains or AD Forests. If you experience delays when searching for or authenticating users, this may be due to a complex directory structure. You can integrate directly with the global catalog to query multiple forests using one Lightweight Directory Access Protocol (LDAP) endpoint for better results. To do this, configure the following settings:
 - **Encryption Type** = None
 - **Port** = 3268
 - Verify that your firewall allows for this traffic on port 3268.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Enterprise Integration / Email (SMTP)

The Simple Mail Transfer Protocol (SMTP) is a protocol for sending email messages between servers. Configure the settings on this page if you are using this protocol for sending emails from the Workspace ONE UEM console to the enrolled device users.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Server	Enter the address of the SMTP server.
Enable SSL	Select to enable Secure Socket Layer security for the email communication.
Port	Enter the port value. The default port for SMTP server is 25.
Requires Credentials	Select to enable basic authentication for sending outgoing mails. Then, enter the Username and Password of an account that has the permission to send outgoing mails in the applicable fields.
Timeout in Seconds	Enter the time (in seconds) that the Workspace ONE server awaits response from the SMTP server after which the session expires.

Setting	Description
Sender's Name	Enter the display name for the outgoing mails.
Sender's Email Address	Enter email address for sending outgoing mails.

- **Test Connection** – Select this to check if Workspace ONE is able to communicate with the SMTP server that you have entered in the above field.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Enterprise Integration / VMware Tunnel / Configuration

The VMware Tunnel configuration page is used to configure fundamental Tunnel architecture to establish connectivity and trust within your environment.

VMware Tunnel offers secure method for individual applications to access corporate resources. VMware Tunnel authenticates and encrypts traffic from individual applications on compliant devices to the back-end system they are trying to reach. VMware Tunnel serves as a relay between your mobile devices and enterprise systems by authenticating and encrypting traffic from individual applications to back-end systems.

Note If you already have EIS configured then you need to disable it by unchecking its check box on the EIS settings page. See [System / Enterprise Integration / Enterprise Integration Services](#).

System / Enterprise Integration / Tunnel / Network Traffic Rules

The Network Traffic Rules settings page enables you to create traffic rules to control how the Per App Tunnel works on supported devices. The rules set on this page determine how the VMware Tunnel handles network traffic from configured Per App VPN mobile applications.

Traffic can be blocked from specified domains, tunneled through to your internal network, bypass your internal network, or directed to a proxy.

System / Enterprise Integration / Third Party Proxies

The Third Party Proxies settings page lets you configure an F5 or standard proxy for the SDK enabled apps.

System / Enterprise Integration / Peer Distribution / Peer Distribution Software Setup

The Peer Distribution Software Setup settings page is used to download and configure the peer-to-peer server.

For more information on Peer Distribution setup, configuration, and installation see [Peer Distribution for Win32 Applications](#).

System / Enterprise Integration / CDN / Akamai

The CDN system settings pages lets on-premises customers enter account information for the available CDN providers. This feature is automatically configured for SaaS customers.

This feature lets end users in different regions download internal applications from the CDN server closest to them, as opposed to an internal file server located remotely. Benefits include increased download speeds for end users and reduced bandwidth for your Workspace ONE servers.

This integration requires that you have an account with the applicable CDN provider. The values on this page can be retrieved by logging in to your CDN provider portal, locating the values, and enter them in this page. If you are an on-premises customer who requires additional assistance, contact Workspace ONE UEM Support.

System / Enterprise Integration / Pull Service Installers

The Pull Service Installers setting page contains links to pull service installers that you can download and run for use in product provisioning.

For more information about pull service installers and their function, please refer to one of the many Workspace ONE UEM product provisioning platform guides, which includes QNX, Windows Rugged, Android Rugged, Windows 7 and macOS.

System / Enterprise Integration / SMS

Complete the fields on this page to enable Workspace ONE UEM to communicate using SMS with mobile devices for purposes such as user or device activation messages.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
SMS	Select to enable Workspace ONE UEM to send short message service (SMS) messages to supported devices.
Gateway Type	Select the SMS Gateway you would like to use. Settings may change based on your selection. Not all settings are documented below.

Setting	Description
Nickname	Enter the nickname for the SMS Gateway Account.
Username	Enter the username used to authenticate the sender with the SMS provider.
Password	Enter the password to complete the authentication of the sender with the SMS provider.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Enterprise Integration / Syslog

The Syslog settings page lets you configure integration with a SIEM tool that leverages the syslog protocol to record system events.

Security Information and Event Management (SIEM) technology gathers information about security alerts generated by network hardware and software components. It centralizes this data and generates reports to help you monitor activity, perform log audits, and respond to incidents. Workspace ONE UEM integrates with your SIEM tools by sending event logs using Syslog.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

General Tab

Setting	Description
Syslog Integration	Enable or disable syslog integration.
Host Name	Enter the URL for the SIEM tool in the Host Name text box.
Protocol	Select the required protocol from available options to send the data. It is to be noted that support for TLS v1.1 is provided.
Port	Enter the port number to communicate with the SIEM tool in the Port text box.
Syslog Facility	Select the facility level for the feature from the Syslog Facility menu. The syslog protocol defines the syslog facility. The widespread use and manipulation of the syslog protocol can clutter the meaning of the syslog facility. However, it can roughly suggest from what part of a system a message originated and it can help distinguish different classes of messages. Some administrators use the syslog facility in rules to route parts of messages to different log files.
Message Tag	Enter a descriptive tag to identify events from the Workspace ONE UEM console in the Message Tag text box. For example, "AirWatch".
Message Content	Enter the data to include in the transmission in the Message Content text box. This is how the message data gets formatted when sent using syslog to your SIEM tool. Use lookup values to set the content. For secure TCP, New line (CRLF) formatting using Enter, \n, \r does not work and gets automatically converted to tab, \t for secure TCP.

Advanced Tab

Setting	Description
Console Events	Select whether to enable or disable the reporting of Console events.
Select Console Events to Send to Syslog	<p>Visible if you enable Console Events. For each sub-heading, select the specific events that you want to trigger a message to syslog.</p> <p>Use Select All or Clear All to select or unselect all the events all at once. To select or unselect specific events, enable or disable the checkboxes.</p> <p>Note On enabling the Console Events, by default, all events under all categories of console events are selected.</p>
Device Events	Select whether to enable or disable the reporting of Device events.
Select Device Events to Send to Syslog	<p>Visible if you enable Device Events. For each sub-heading, select the specific events that you want to trigger a message to syslog.</p> <p>Use Select All or Clear All to select or unselect all the events all at once. To select or unselect specific events, enable or disable the checkboxes.</p> <p>Note On enabling the Device Events, by default, all events under all categories of device events are selected.</p>

- **Test Connection** – Use the **Test Connection** button to ensure successful communication between the Workspace ONE UEM console and the SIEM tool.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Enterprise Integration / Remote Management

The Remote Management settings page lets you configure the Remote Management Server. This page is used during the setup of the Remote Management Server version 3 only.

Administrators of Workspace ONE Assist, previously known as Advanced Remote Management, should refer to the **Workspace ONE Assist** documentation, available at docs.vmware.com.

System / Enterprise Integration / VMware Identity Manager

The VMware Identity Manager settings page is used to complete the VMware Identity Manager Configuration and Access Management.

Identity Manager Configuration

[System / Enterprise Integration / VMware Identity Manager/ Configuration](#)

Identity Manager Access Management

[System / Enterprise Integration / VMware Identity Manager/ Access Management](#)

System / Enterprise Integration / VMware Identity Manager/ Configuration

The VMware Identity Manager configuration setting is used to configure directory integration settings between your Workspace ONE UEM instance and your Identity Manager instance.

After binding the two together, Identity Manager can make API calls related to your directory service values. Workspace ONE UEM customers must first deploy VMware Enterprise Systems Connector and set up directory service integration within the Workspace ONE UEM console. Then, you can use this settings page to push your directory configuration to Identity Manager. This functionality does not allow for Workspace ONE UEM to receive directory changes from Identity Manager.

For more information about integrating Workspace ONE UEM with Identity Manager and deploying Workspace ONE with single sign-on to devices, see the Workspace ONE Quick Configuration Guide.

System / Enterprise Integration / VMware Identity Manager/ Access Management

With Workspace ONE, you can easily control access to your catalog and applications. With VMware Identity Manager, you can configure authentication methods, identity provider instances, default access policy rules, and network ranges.

Every time a user attempts to log in, VMware Identity Manager evaluates the default access policy rules that you have set which determines the rules that must be applied. Authentication methods are always applied in the order that you have listed within the rule. The first identity provider instance that meets the authentication method and network range requirements of the rule is applied. The user authentication request is then forwarded to the identity provider instance for authentication. If the authentication fails, then the next configured authentication method in the rule is applied.

As an administrator, if you click **Access Management** without configuring the integration between the VMware Identity Manager and Workspace ONE UEM, you are prompted to complete the configuration.

Click **Configure** to initiate the configuration. The Access management screen allows you to configure the **Authentication Methods**, **Identity Providers** and **Access Policies** in the VMware Identity Manager.

- 1 Click **Authentication Methods** to configure user authentication in VMware Identity Manager. For more information, see **Managing Authentication Methods to Apply to Users** in <https://docs.vmware.com/en/VMware-Identity-Manager/index.html>.
- 2 Click **Identity Providers** to associate the authentication methods to use in the built-in identity provider. For more information, see **Using Built-in Identity Providers** in <https://docs.vmware.com/en/VMware-Identity-Manager/index.html>.

- Click **Access Policies** to provide secure access to the users apps portal and to start Web and desktop applications. For more information, see **Managing Access Policies** in <https://docs.vmware.com/en/VMware-Identity-Manager/index.html>.

Note Workspace ONE UEM and VMware Identity Manager use password-grant work flow that allows access to VMware Identity Manager from Workspace ONE UEM with single sign-on (SSO). For more information, see [Single Sign-On to VMware Identity Manager from Workspace ONE UEM](#).

Single Sign-On to VMware Identity Manager from Workspace ONE UEM

Workspace ONE UEM and VMware Identity Manager use password-grant work flow that allows access to VMware Identity Manager from Workspace ONE UEM with single sign-on (SSO).

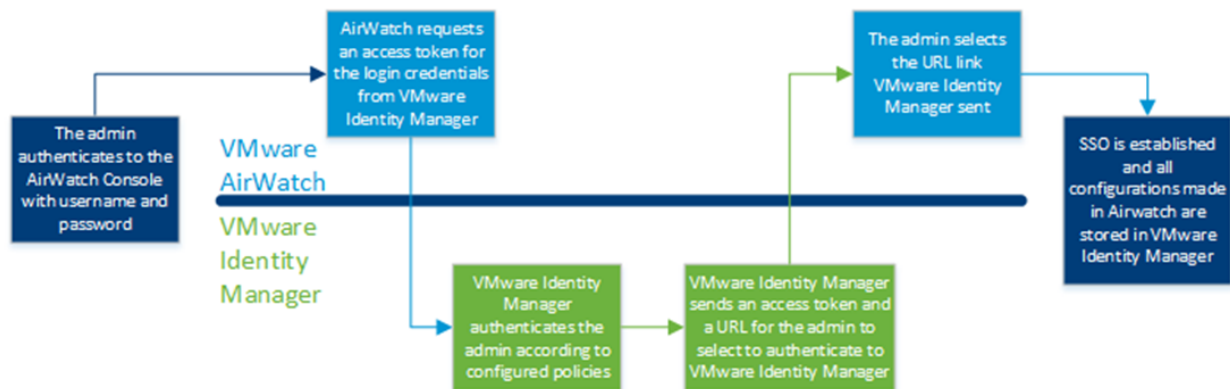
The configuration settings are in VMware Identity Manager and not in Workspace ONE UEM. The exception to this process is configurations made in SaaS applications and access policies.

Requirements

The admin must have administrative roles in both Workspace ONE UEM and VMware Identity Manager.

Workflow

VMware Identity Manager and Workspace ONE UEM work in the back-end to authenticate the Workspace ONE UEM admin to VMware Identity Manager. Admins authenticate to Workspace ONE UEM with their usernames and passwords. This username and password triggers a request for an access token from VMware. After SSO is established, all configurations made in Workspace ONE UEM are stored in VMware Identity Manager.



System / Security / Restricted Actions

The Restricted Actions settings page lets you configure security-minded settings related to the actions that administrators can perform in the Workspace ONE UEM console.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Send Message to All

- **Enabled** – Enable this setting to allow a System Administrator to send a message to all devices in your deployment from the Device List View.

Password Protect Admins

You can require that certain actions require admins to enter a PIN. For each action you choose to protect, select the appropriate **Password Protect Actions** button for **Enabled** or **Disabled** as appropriate. This requirement provides you with granular control over which actions you want to make more secure.

Note Some actions always require a PIN and as a result cannot be disabled. Denoted by * following.

You can set the maximum number of failed attempts the system accepts before automatically logging out the session. If you reach the set number of attempts, you must log into the Workspace ONE UEM console and set a new security PIN.

Setting	Description
Admin Account Delete	Prevents the deletion of an admin user account in Accounts > Administrators > List View .
*Regenerate VMware Enterprise Systems Connector Certificate	Prevents the regeneration of the VMware Enterprise Systems Connector certificate in Groups & Settings > All Settings > System > Enterprise Integration > VMware Enterprise Systems Connector .
*APNs Certificate Change	Prevents the disabling of APNs for MDM in Groups & Settings > All Settings > Devices & Users > Apple > APNs For MDM .
Application Delete/Deactivate/Retire	Prevents the deletion, deactivation, or retirement of an application in Apps & Books > Applications > List View .
Content Delete/Deactivate	Prevents the deletion or deactivation of a content file in Content > List View .
*Data Encryption Toggle	Prevents the Encryption of user information setting in Groups & Settings > All Settings > System > Security > Data Security .
Device Delete	Prevents the deletion of a device in Devices > List View . Admin security PIN is still required for bulk actions even when this setting is disabled.
*Device Wipe	Prevents any attempt to perform a device wipe from the Device List View or Device Details screens.
Enterprise Reset	Prevents any attempt to perform an enterprise reset on a device from the Devices Details page of a Windows Rugged, Rugged Android, or QNX device.
Enterprise Wipe	Prevents any attempt to perform an enterprise wipe on a device from the Devices Details page of a device.
Enterprise Wipe (Based on User Group Membership Toggle)	Prevents any attempt to perform an enterprise wipe on a device when it is removed from a user group. This setting is an optional setting that you can configure under Groups & Settings > All Settings > Devices & Users > General > Enrollment on the Restrictions tab. If you Restrict Enrollment to Configured Groups on this tab, you then have the added option of performing an enterprise wipe a device when it is removed from a group.
*Organization Group Delete	Prevents any attempt to delete the current organization group from Groups & Settings > Groups > Organization Groups > Organization Group Details .
Profile Delete/Deactivate	Prevents any attempt to delete or deactivate a profile from Devices > Profiles & Resources > Profiles .

Setting	Description
Provisioning Product Delete	Prevents any attempt to delete a provisioning product from Devices > Staging & Provisioning > Products List View .
Revoke Certificate	Prevents any attempt to revoke a certificate from Devices > Certificates > List View .
*Secure Channel Certificate Clear	Protects from any attempt to clear an existing secure channel certificate from Groups & Settings > All Settings > System > Advanced > Secure Channel Certificate .
User Account Delete	Prevents any attempt to delete a user account from Accounts > Users > List View .
Change in Privacy Settings	Prevents any attempt to alter the privacy settings in Groups & Settings > All Settings > Devices & Users > General > Privacy .
Delete Telecom Plan	Prevents the deletion of a telecom plan in Telecom > Plan List .
Override Job Log Level	Prevents attempts to override the currently selected job log level from Groups & Settings > Admin > Diagnostics > Logging . Overriding the Job Log Level is useful when a device or group of devices is having an issue. In this case, the admin can override those device settings by forcing an elevated log level to Verbose, which logs the maximum level of console activity, making it ideal for troubleshooting.
*App Scan Vendor Reset/Toggle	Prevents the resetting (and subsequent wiping) of your app scan integration settings. This action is performed in Groups & Settings > All Settings > Apps > App Scan .
Shut Down	Prevents any attempt to shut down the device in Devices > List View > Device Details .
Maximum invalid PIN attempts	Defines the maximum number of invalid attempts at entering a PIN before the console locks down. This setting must be between 1 and 5.

Required Notes for Action

You can also require admins to enter notes using the **Require Notes** check box and explain their reasoning when performing these actions.

Setting	Description
Lock Device	Require a note for any attempt to lock a device from Device List View or Device Details .
Lock SSO	Require a note for any attempt to lock an SSO session from Device List View or Device Details .
Device Wipe	Require a note for any attempt to perform a device wipe from Device List View or Device Details .
Enterprise Reset	Require a note for any attempt to enterprise reset a device from the Device Details page of a Windows Rugged or Rugged Android device.
Enterprise Wipe	Require a note for any attempt to perform an enterprise wipe from Device Details .
Override Job Log Level	Require a note before attempts to override the default job log level from Groups & Settings > Admin > Diagnostics > Logging .
Reboot Device	Require a note before a reboot attempt from Devices > List View > Device Details .
Shut Down	Require a note before a shut down attempt from Devices > List View > Device Details .

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Security / Data Security

The Data Security settings page lets you encrypt user information to further secure your user data, which includes an end user's first name, last name, email, and phone number.

Enabling this feature limits some Workspace ONE UEM functionality, such as search, sort and filter. Consider the implications carefully before enabling this feature.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Encrypt User Information	Select Enabled and then select each user data field you would like to encrypt. Encrypting a field means it will not display in other parts of the Workspace ONE UEM console. However, doing so also disables search, sort and filter on the items selected.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Security / SSL Pinning

The SSL Pinning settings page is where you can add domains of Workspace ONE UEM Device Services and auxiliary components, which can help prevent man-in-the-middle (MITM) attacks by enabling an additional layer of trust between the listed hosts and devices.

The certificates and domains you add here serve as a trusted form of validation that functions in addition to the standard certificate check a device performs against a Workspace ONE UEM component server. When devices establish sessions with your Workspace ONE UEM component servers, they also check the certificate against this stored certificate to guard against MITM attacks.

When you first navigate to this page, the Device Services site URL displays. However, no certificate data is present until you upload a certificate.

Important The SSL pinning feature is only functional if it is used in conjunction with a Workspace ONE UEM application that supports certificate pinning.

Setting	Description
On/Off	Enable or disable pinning using this switch. If you turn pinning from on to off, it terminates all pinning at the current organization group and all the child organization groups underneath it.
Upload (under Device Services)	Select this button in the Device Services section of the page to add the Hostname and upload the certificate used for validation. If you have load-balanced Device Services servers, you also need to upload the certificates for each server. You will not see this button if you already have a device services certificate populated.

Setting	Description
Sync	After uploading your Device Services certificate, you need to select Sync to initiate pinning. After, the sync status changes to a green color to indicate pinning was successful and the page should display your synced pin list.
Add Host (under auxiliary)	<p>Select to add auxiliary components other than Device Services that you also want to enable pinning for. On the Add Pinned Host dialog, enter the following:</p> <ul style="list-style-type: none"> ■ Host – Enter the fully qualified domain name of the host. ■ Required – Select to require the certificate pin to be pinned at all child organization groups and prevent it from being disabled or modified by child organization group administrators.
Upload (under auxiliary)	Select to upload the certificate used for validation for each of your auxiliary components.

System / Security / SSL Pinning / Requirements

Software Requirements

- AirWatch App with SSL pinning support

Note iOS devices enrolled using Web enrollment and DEP enrollment do not support certificate pinning during the enrollment process.

- List of certificates that devices may encounter when connecting to Device Services (DS)

Note Necessary certificates may include a Load Balancer certificate.

Network Requirements

- On-premises customers will need to install an on-prem instance of the Trust Service.
- On-premises customers can configure a load balancer or reverse proxy configuration. The only requirement is that the path that hosts Trust Service serves up the custom SSL cert you get from myWorkspaceONE. You can decide if offloaded or passthrough works best for your deployment.

System / Security / SSL Pinning / Configure

Configure your Workspace ONE UEM deployment to accept SSL certificate pinning.

SSL configuration is only required if you are unable to leverage the AWCM Trust Service. If you are in an on-premises environment leveraging the AWCM Trust Service, proceed to [Upload SSL Device Services Certificate](#).

Prerequisites

- Configure the Workspace ONE Hub with SSL pinning support.

Note iOS devices enrolled using Web enrollment and DEP enrollment do not support certificate pinning during the enrollment process.

- Gather a list of certificates that devices may encounter when connecting to Device Services (DS). Necessary certificates may include a Load Balancer certificate.
- Configure an On-Premises Trust Service (TS) or a network exception. On-Premises customers should install an on-premises instance of the Trust Service.
- If you have a closed-network deployment, set up a network exception to the Cloud Trust Service, which is hosted on the Auto-Discovery domain (discovery.awmdm.com)

Procedure

- 1 In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > Admin > Cloud Services > Workspace ONE ID**. Select **Workspace ONE ID for Auto Discovery Mode** and use your Workspace ONE ID to generate the HMAC Token.

When the token generates, verify that the appropriate firewall rules are configured.

Table 2-1. HMAC Token Firewall Configuration

Source	Port	Destination
Workspace ONE UEM console	TCP 443 (TLS)	discovery.awmdm.com
Device Services	TCP 443 (TLS)	discovery.awmdm.com
discovery.awmdm.com	TCP 443 (TLS)	Device Services
Devices	TCP 443 (TLS)	discovery.awmdm.com (or on-premises Trust Service)

- 2 Install the Trust Service software on an on-premise server. This can be on a stand-alone server, or on a server with other Workspace ONE applications, such as Device Services.
- 3 Provision a certificate for the Trust Service that is signed by the Workspace ONE UEM signing service.
 - a Create a Certificate Signing Request (CSR) for the server where you are installing the Trust Service in a normal manner.
 - The CSR should have an email address designated to it, with a domain that matches the domain of the MyWorkspaceONE ID requesting the certificate from MyWorkspaceONE.
 - The CSR cannot have multiple DNS names in the **Subject Alternative Name**.
 - b Generate a signed certificate in myWorkspaceONE by navigating to **My Company > Certificate Signing Portal > Sign a Certificate** and paste and **Submit** the signing request content from the CSR file you created in the first step.
 - c **Download** the newly-signed certificate .cer file.

- 4 Bind the certificate downloaded from myWorkspaceONE to all servers with the Trust Service application.

In an environment leveraging a load balancer or a reverse proxy, the certificate may need to be bound to those components as well to ensure a device can establish a secure connection.

Note If the Trust Service is installed on an existing server (such as a Device Services server), this certificate should be bound to a unique port on that server. Trust Service cannot use the same port as another server application.

- 5 In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Security > Trust Service**. Insert the Trust Service URL (specifying the port if necessary, such as `https://<host>:<port>/TrustService`) and select **Save**.
- 6 Verify that you can hit the service (`https://<host>:<port>/TrustService/sslpinning/settings?URL=<host>`).

What to do next

Upload the Device Services Certificate you have configured to the Workspace ONE UEM console using [Upload SSL Device Services Certificate](#).

Upload SSL Device Services Certificate

Complete the SSL certificate pinning by uploading the certificate to the Workspace ONE UEM console.

Prerequisites

Configure the SSL certificate for your deployment as described in [System / Security / SSL Pinning / Configure](#).

Procedure

- 1 In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Security > SSL Pinning**.

- 2 Under **Device Services**, select **Upload**.

- 3 Select **Choose** file. Locate the file containing the public key of the certificate bound to the Device Services server endpoint.

If you do not have access to the DS server to retrieve the public key of the bound certificate, most web browsers will allow you to save the public key of a website you visit. The steps to do so will vary depending on the browser you use, but once you view the certificate, you can select **Details > Copy to File...** or **Details > Export** and save the file locally.

- 4 Select **Enter** to upload and then **Submit** the certificate key.

- 5 If the environment is leveraging the AirWatch Cloud Trust Service, select **Sync**. A successful sync is indicated by a green light and a synchronized message indicating the certificate has synced to the Cloud SSL Pinning service.

The sync button pushes the configured DS certs up to the cloud “Trust Service” that lives in Auto Discovery. If the sync button fails, then Auto Discovery will not return the pins they have added and the device may not pin the connection.

Note If you are using an on-premises Trust Service, you do not have to Sync the certificate.

Results

Your device services certificate is uploaded.

System / Security / Trust Service

The Trust Service page is for use by on-premises administrators and can only be configured at the Global level. In general, you should contact Workspace ONE UEM if you want to learn more about this feature or believe it may be required for your deployment, as it involves certificate signing workflows and external downloads from myAirWatch.

The Trust Service is a secure way to disable SSL pinning for closed network, on-premises deployments where devices do not have outbound access to the Workspace ONE UEM public cloud. In this case, a trust service must be installed if Workspace ONE UEM mobile applications that support SSL Pinning will be used as they will not be functional otherwise. The Trust Service serves as a root of trust to notify devices that they are not to attempt communication with the Workspace ONE UEM Cloud and can proceed without the need to retrieve pinned SSL Certificates from Workspace ONE UEM hosted services. The Trust Service must use a custom SSL certificate signed by a Workspace ONE UEM root certificate to establish trust with the device.

System / Security / Key Management

The Key Management settings page lets on-premises customers rotate the master key used to encrypt sensitive data in the Workspace ONE UEM database.

The factors of this encryption are split between the database, where the master key resides, and the application servers, where a separate key encrypting key (KEK) resides. Configuring this feature is a multi-step process that requires access with administrator permissions to all Workspace ONE UEM servers and system administrator privileges at the global-level organization group in the Workspace ONE UEM console.

Setting	Description
Passphrase / Confirm Passphrase	Enter and confirm a strong passphrase. You must remember this passphrase for future use.
Generate	Select this button to generate the KEK and the master key. Selecting this option reveals the Installation File and Download button.

Setting	Description
Download	Select to download the install.config file. After you download this file, you have 48 hours to complete the next step, as after this time the master key will be active.
Abort	Select this button if something goes wrong, such as losing or forgetting the passphrase, and the rotation must be aborted. You can do so provided the abort happens before the 48 hours. After 48 hours, the rotation cannot be aborted. Be sure to keep the passphrase safe, as recovering data that has been encrypted with the new, rotated key after 48 hours is not possible.
Recover	In some cases you may see a Recover button next to Abort, indicating that the configuration file may have expired. In this case, you do not need the passphrase to abort.

Next Steps

Using the install.config file from the UEM console, install the KEK to all Workspace ONE UEM servers using the Key Installation Utility. To do this, execute the following command on each Workspace ONE UEM Server:

```
Utility.exe -f /path/to/install.config
```

If install.config is in the same directory as the utility, all command-line arguments can be omitted. After you run these commands, the installation completes.

System / Help

The Help settings page lets you configure the help settings for the Workspace ONE UEM console.

Setting	Description
Enable Help	Enable or disable the help icon to access help in the upper right corner of the UEM console.
Help Skin Name	The name of the help skin name. This value should be left as-is.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Localization / Language Activation

The Language Activation page allows administrators to offer localized interaction with the Workspace ONE UEM console through the use of globalized message templates, EULAs and more. This allows administrators to offer a tailored, global experience to all of their users, regardless of language preference or location. Enable the desired languages, then assign it as the default locale of an organization group for all users to see content in that language by default.

System / Localization / Localization Editor

The **Localization Editor** allows administrators to personalize UI text in the system to match internal word choice or regional preferences for all users.

Use the **Override** option to ensure that corporate language, such as specific technical operations or company structure, are displayed instead of default values in the Workspace ONE UEM console.

If you want to make a large number of customizations to the labels in the UEM console, you can make bulk changes to label content. To make bulk changes to labels, take the following steps.

Procedure

- 1 Navigate to **Groups & Settings > All Settings > System > Localization > Localization Editor**.
- 2 Select the **Modify** button. The **Modify Label Content** screen displays.
- 3 Select the **Locale** language from the drop down menu.
- 4 Select the **Download** button to save a CSV (comma separated values) template to a local storage space on your device.
- 5 Open this file with Excel and make your changes to it, saving your changes at the conclusion.
- 6 In the **Modify Label Content** screen, select the **Choose File** button and locate the saved CSV template on your device.
- 7 Select the **Upload** button. The customizations you made to the CSV file are applied to your Workspace ONE UEM deployment.

Note Device side label updates take effect after the Internet Information Service (IIS) app pool refreshes on your Device Services server.


What to do next

You can revert any localization changes made back to its original state.

- 1 Select the label key you want to revert by clicking its check box.
- 2 Select **Revert**.

System / Report Subscriptions

The **Report Subscriptions** system setting is simply a listing of the Reports you can subscribe to through the Hub. Navigate to the Report Listing using **Hub > Reports & Analytics > Reports > List View**.

When you select the **Subscribe** button  on one or more reports in the listing, you elect to receive this report daily, weekly, monthly, or just a single occurrence. You may also optionally include other email addresses in the subscription.

Once you have subscribed to one or more reports in the **Hub**, you will be able to view these reports listed in **System > Reports & Alerts > Report Subscriptions**. You are also able to edit the subscription details such as:

■ Organization Groups	■ User
■ Date	■ Optional Email Addresses
■ Recurrence	■ Distribution List
■ Role	

System / Terms of Use

The Terms of Use settings page lets you configure terms of use for the Workspace ONE UEM console, enrollment, and apps.

Ensure that all users with managed devices agree to the policy by defining and enforce terms of use (TOU). If necessary, users must accept the TOU before proceeding with enrollment, installing apps, or accessing the UEM console. The UEM console allows you to customize fully and assign a unique TOU to each organization group and child organization group.

System / S/MIME

S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending email. This protocol allows to encrypt emails and digitally sign them, thus allowing the receiver to be certain that the message received is exact and has been sent by a specific sender.

Configure the below settings to enable S/MIME and deploy it on devices through profiles.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Retain S/MIME Certificate	Select to retain and enable S/MIME certificate deployment through the profile.
Temporary S/MIME Retention Period (hours)	Enter time (in hours) to retain the S/MIME certificate only for a limited duration.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / Hub URLs

This page is used to specify your Workspace ONE Intelligent Hub schema and default URLs referenced during the enrollment process to obtain the Workspace ONE Intelligent Hub. These settings typically do not need to be modified.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Public Store URLs

Setting	Description
iOS Public App Store URL	App Store URL that is used when downloading the iOS Hub during the enrollment process.
Android Public App Store URL	Google Play store URL that is used when downloading the Android Hub during the enrollment process.

Hub Schema

Setting	Description
iOS Hub Schema	Handler used to identify the iOS Hub that will be opened during enrollment.
Android Hub Schema	Handler used to identify the Android Hub that will be opened during enrollment.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / API / Event Notifications

The Event Notification setting page is used to configure the settings for event notifications to capture specific device-related events in real time. Workspace ONE UEM event notifications use HTTP URLs and the basic user method of authentication. Workspace ONE UEM supports notifications for specific events using Webhooks/Event Notification.

Webhooks are HTTP callbacks, sent to the URL of your choosing whenever the specified event occurs. You provide the URL as the callback destination after subscribing to the particular event. Additionally, because callbacks are returned to the specified URL every time an applicable event occurs, you do not need to regularly poll the server for event information.

The Event Notification log file is called `ChangeEventOutboundQueueService.Log` and it can be found in the `Logs/Services` folder where Workspace ONE UEM is installed.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

To add an event notification, navigate to **Groups & Settings > All Settings > System > Advanced > API > Event Notifications**, select the **Add Rule** button, and complete the following settings.

Setting	Description
Target Name	This is the label for the event notification. You can see this entry in the Event Notifications page.
Target URL	Enter the target URL which is configured to receive the webhook callback.
User Name	Enter the Workspace ONE UEM user name.
Password / Confirm Password	Enter and confirm the password that corresponds to the Workspace ONE UEM user name.
Format	Select the format for the webhook callback: JSON or XML.

You can configure notification settings for the following events.

Setting	Description
Check-in/Check-out	Send a notification when a multi-user device is checked-in or checked-out.
Device Attribute Change	Enable to activate the Device Attribute submenu, making it possible to enable individual device identifiers to trigger a notification when they are altered.
	Asset Number
	Device Friendly Name
	Device MCC
	Ownership
	Organization Group ID
	Operating System
	Phone Number
	User Email Address
Device Compliance Status Change	Send a notification when the compliance status of a device changes.
Device Compromised Status Change	Send a notification when the compromised status of a device changes, specifically when an Android device is "rooted" or when an iOS device is "jailbroken".
Device Delete	Send a notification when a device is deleted from Workspace ONE UEM.
Device Enrollment	Send a notification when a device enrolls into either the Workspace ONE Intelligent Hub or Workspace ONE UEM.

Setting	Description
Device Unenrolled Enterprise Wipe	Send a notification when a device is enterprise wiped.
Device Wipe	Send a notification when a device is wiped.

For more information on detailed configuration part, refer to **VMware AirWatch API Event Notification Guide**, available on docs.vmware.com.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / API / REST API

APIs require authentication to integrate with Workspace ONE UEM. Prior to authentication, API access must be enabled in the Workspace ONE UEM console. This page is used to configure the settings required for REST APIs.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

General Tab

Setting	Description
Enable API Access	Select Enable API Access for APIs to integrate with Workspace ONE UEM. APIs get authenticated (either basic authentication or directory authentication) to integrate Workspace ONE UEM only if this check box is enabled.
Add	<p>Select Add to add/or generate multiple API keys.</p> <ul style="list-style-type: none"> ■ Service – Enter one or multiple service(s) and generate their own independent API keys. ■ Account Type – Select the type of the account. To access Personal Content APIs (MCM APIs), select the Account type as Enrollment User. ■ API Key – Read-only key generated when you select the Add button. ■ Description – Enter short description for the service and generated API key. ■ Whitelisted Domains – Enter domains that can interact with Workspace ONE UEM APIs through the API key. ■ Admin Generated? – Displays which API keys were automatically generated and which were manually generated for different integrations.

Authentication Tab

Setting	Description
Basic	Select basic access for authentication using basic credentials (username and password). Credentials only exist in Workspace ONE UEM and do not necessarily match the existing corporate credentials. It requires no technical integration and no enterprise infrastructure.
Certificates	<p>Certificate-based API authentication is utilized to provide the API access to the admin users. Utilizing this method, a self-signed, user-level API certificate must be generated from the Workspace ONE UEM console.</p> <p>Note Disabling certificate based authentication breaks any existing integration with other services that rely upon it such as GreenBox, Access (formerly vIDM), Tunnel, Tunnel Proxy, SEG, and so forth, causing those services to fail. If you want to disable certificate based authentication, you must first make certain that no running service depends upon it.</p>
Directory	Select directory access of authentication if you want to integrate user and admin accounts of Workspace ONE UEM with existing corporate accounts. End users now authenticate with existing corporate credentials.

Usage Tab

Setting	Description
Server Throttling	<p>Set the server bandwidth throttling (calls per minute). When the server reaches the specified throttling limit, it offloads new requests and does not respond to them. The default value is 5,000.</p> <p>If you set the calls-per-minute to 0, the throttling is turned off and you can make an unlimited number of API calls.</p>
Daily Quota	<p>Set the number of API calls to be sent per day. The default value is 50,000. If your calls-per-day is 0, no API calls connect.</p> <p>Note Increasing the maximum value can potentially lead to the server performance issue. Contact Workspace ONE support if needed.</p>
Daily Quota Usage	Specifies the number of the API calls used out of the daily quota set for the API calls.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / API / SOAP API

This page is used to configure the settings required for SOAP APIs.

Setting	Description
Subject	Enter the name of the individual , computer, device, or certificate authority to whom the certificate is issued.
Thumbprint	The thumbprint of API certificate.
Date Issued	The date certificate was last created.

Setting	Description
Clear Client Certificate	Click to clear the existing certificate and its data.
Export Client Certificate	Click to download and store the certificate in .P12 format.

System / Advanced / Device Root Certificate

The Device Root Certificate settings page contains information for the certificate of the same name, which is used to authenticate SDK-enabled apps that require certificate-based authentication.

System / Advanced / Secure Channel Certificate

The Secure Channel Certificate settings page lets you configure options related to the certificate of the same name.

For on-premises customers, the Secure Channel Certificate establishes a trust between Workspace ONE UEM and any components (e.g. VMware Enterprise Systems Connector, AWCM) that are installed on premises. VMware Enterprise Systems Connector automatically packages this certificate in its installer, but for AWCM you will need to download it from here.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Block Non-Secure Channel Device Access

Select a check box next to each of the platforms with which you want to enforce communication with the Workspace ONE UEM console over a secure channel.

AirWatch Cloud Messaging

Download AWCM Secure Channel Certificate Installer – Downloads an .exe file that you can run on your AWCM server.

Download CNS Secure Channel Certificate Installer – Downloads a .tar file that you can run on your Cloud Notification Service server. The Secure Channel Installer for Linux is only used for the Cloud Notification Service. AWCM is only supported on Windows servers.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / Service URLs

The **Service URLs** settings page is the place you define your Identity Management Provider (IdM) to Workspace ONE UEM. The IdM describes the management of individual identities, their authentication, authorization, roles and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks.

There can only be one IdM per organization group and when the **Override** setting is enabled, the Identity Management Provider for each nested OG in your Workspace ONE UEM deployment can be unique. This means you may have several IdMs to keep track of.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Identity Management Provider

Setting	Description
Name	Enter the name of the Identity Management Provider. This field is required.
URL	Enter the URL of the Identity Management Provider. This field is required.
Username	Enter the username with which the Identity Management Provider can identify you.
Password	Enter the password with which the Identity Management Provider will authenticate you.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / Site URLs

The Site URLs settings page lists the endpoints of the various components that comprise the Workspace ONE UEM solution.

Typically, the settings on this page never change, and you should not alter them unless instructed to do so by Workspace ONE UEM.

Certain functionality, such as the Remote Tunnel Server for rugged devices and App Wrapping for your internal apps, can be enabled on this page.

You can also configure your AWCM server URLs and port from this page.

System / Advanced / Query String Authentication

A query string authentication provider is a non-SAML service that allows users to log in to a web portal, select a web service or application, and automatically be authenticated and signed in without having to re-enter credentials.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Enable Query String Authentication	Select to enable the feature.
Parameter Name	<p>Enter the query string parameter name in the Parameter Name field. This must be a single value – multiple parameter names are not supported. This is the value that Workspace ONE UEM uses to recognize the login request.</p> <p>This parameter name comes from your query string authentication provider. Consult your authentication provider for instructions on retrieving this information.</p>
Session Validation URL	Enter the URL of the query string authentication provider instance. It is used for session validation and administrator account details retrieval. If needed, you can include a port number for network traffic as part of the URL.

An example of the login request to the Workspace ONE UEM console would be: `https://acme.mdm.com/login?<Parameter>=<session_ID>`, where `acme.mdm.com` is the URL of your UEM console, `<Parameter>` is the parameter name, and `<session_ID>` is the session ID passed from the query string authentication provider to Workspace ONE UEM for authentication.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

System / Advanced / Other

The Advanced / Other settings page contains a number of legacy settings for earlier versions of Workspace ONE UEM that have been omitted. With the exception of the **two settings below**, do not alter these settings unless you know what they do and are instructed to do so by Workspace ONE UEM support.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Display Select Language on Login Page	Displays a Select Language drop-down on the Workspace ONE UEM console login page.
Display What's New Popup	Displays the What's New popup when admins log in to the Console. Admins can opt to not show this message on subsequent logins.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users

3

This section provides information about Workspace ONE UEM Devices and Users settings.

The Devices and Users settings are categorized into the following:

- General
- Android
- Apple
- QNX
- Tizen
- Chrome OS
- Windows
- Peripherals
- Advanced

This chapter includes the following topics:

- [Devices & Users / General / Enrollment](#)
- [Devices & Users / General / Friendly Name](#)
- [Devices & Users / General / Lookup Fields](#)
- [Devices & Users / General / Message Templates](#)
- [Devices & Users / General / Notifications](#)
- [Devices & Users / General / Privacy](#)
- [Devices & Users / General / Shared Device](#)
- [Devices & Users / General / Advanced](#)
- [Devices & Users / Android / Android EMM Registration](#)
- [Devices & Users / Android / Hub Settings](#)
- [Devices & Users / Android / Google Play Integration](#)
- [Devices & Users / Android / Auto-Enrollment](#)

- [Devices & Users / Android / Service Applications](#)
- [Devices & Users / Android / Security](#)
- [Devices & Users / Android / Samsung Enterprise FOTA](#)
- [Devices & Users / Apple / APNs for MDM](#)
- [Devices & Users / Apple / Apple iOS / APNs for Applications](#)
- [Devices & Users / Apple / Apple iOS / Hub Settings](#)
- [Devices & Users / Apple / Apple iOS / Managed Settings](#)
- [Devices & Users / Apple / Apple macOS / Hub Application](#)
- [Devices & Users / Apple / Apple macOS / Hub Settings](#)
- [Devices & Users / Apple / Apple macOS / Software Management](#)
- [Devices & Users / Apple / AppleCare](#)
- [Devices & Users / Apple / Automated Enrollment](#)
- [Devices & Users / Apple / MDM Sample Schedule](#)
- [Devices & Users / Apple / Device Enrollment Program](#)
- [Devices & Users / Apple / Profiles](#)
- [Devices & Users / Apple / SCEP](#)
- [Devices & Users / Apple / Install Fonts](#)
- [Devices & Users / Apple / Education](#)
- [Devices & Users / Blackberry / Blackberry 10 / General](#)
- [Devices & Users / Blackberry / Blackberry 10 / Hub Settings](#)
- [Devices & Users / Blackberry / Blackberry 10 / BES 10 Settings](#)
- [Devices & Users / Blackberry / Legacy Blackberry / Hub Settings](#)
- [Devices & Users / BlackBerry / Legacy BlackBerry / BES Settings](#)
- [Devices & Users / QNX / Hub Settings](#)
- [Devices & Users / Tizen / Hub Settings](#)
- [Devices & Users / Chrome OS / Hub Settings](#)
- [Devices & Users / Windows / Windows Auto-Discovery](#)
- [Devices & Users / Windows / Windows Rugged / Hub Application](#)
- [Devices & Users / Windows / Windows Rugged / Hub Settings](#)
- [Devices & Users / Windows / Windows Rugged / Power on Password](#)
- [Devices & Users / Windows / Windows Rugged / Metrics](#)
- [Devices & Users / Windows / Windows Rugged / Advanced](#)

- [Devices & Users / Windows / Windows Phone / Intelligent Hub Application](#)
- [Devices & Users / Windows / Windows Phone / Hub Settings](#)
- [Devices & Users / Windows / Windows Phone / Company Hub Settings](#)
- [Devices & Users / Windows / Windows Phone / MDM Sample Schedule](#)
- [Devices & Users / Windows / Windows Phone / Windows Health Attestation](#)
- [Devices & Users / Windows / Windows 7 / Hub Application](#)
- [Devices & Users / Windows / Windows 7 / Hub Settings](#)
- [Devices & Users / Windows / Windows Desktop / General](#)
- [Devices & Users / Windows / Windows Desktop / Hub Application](#)
- [Devices & Users / Windows / Windows Desktop / Hub Settings](#)
- [Devices & Users / Windows / Windows Desktop / App Deployments](#)
- [Devices & Users / Windows / Windows Desktop / Enterprise Apps](#)
- [Devices & Users / Windows / Windows Desktop / Windows Sample Schedule](#)
- [Devices & Users / Windows / Windows Desktop / Windows Health Attestation](#)
- [Devices & Users / Peripherals / Server](#)
- [Devices & Users / Peripherals / Sample Schedule](#)
- [Devices & Users / Advanced / Bulk Management](#)
- [Devices & Users / Advanced / Custom Fields](#)
- [Devices & Users / Advanced / Device Groups](#)
- [Devices & Users / Advanced / Area](#)
- [Devices & Users / Advanced / Tags](#)
- [Devices & Users / Advanced / User Categories](#)
- [Devices & Users / Advanced / User Migration](#)
- [Devices & Users / Advanced / Unmanaged Device Wipe Protection](#)
- [Devices & Users / Advanced / Managed Device Wipe Protection](#)
- [Devices & Users / Advanced / Profile Options](#)

Devices & Users / General / Enrollment

You can configure several enrollment options related to devices and users. It is divided into several tabs.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Authentication Tab

Setting	Description
Add Email Domain	This button is used for setting up the Auto-Discovery Service to register email domains to your environment.
Authentication Mode(s)	<p>Select the allowed authentication types, which include:</p> <ul style="list-style-type: none"> ■ Basic – Basic user accounts (ones you create manually in the UEM console) can enroll. ■ Directory – Directory user accounts (ones that you have imported or allowed using directory service integration) can enroll. Workspace ONE Direct Enrollment supports Directory users with or without SAML. ■ Authentication Proxy – Allows users to enroll using Authentication Proxy user accounts. Users authenticate to a web endpoint. <ul style="list-style-type: none"> ■ Enter Authentication Proxy URL, Authentication Proxy URL Backup, and Authentication Method Type (choose between HTTP Basic and Exchange ActiveSync).
Source of Authentication for Intelligent Hub	<p>Select the system the Intelligent Hub service uses as its source for users and authentication policies.</p> <ul style="list-style-type: none"> ■ Workspace ONE UEM - Select this setting if you want Hub Services to use Workspace ONE UEM as the source. <p>When you configured the Hub Configuration page for Hub Services, you entered the Hub Services tenant URL.</p> <ul style="list-style-type: none"> ■ Identity Manager - Select this setting if you want Hub Services to use VMware Identity Manager as the source. <p>When you configured the Hub Configuration page for Hub Services, you entered the VMware Identity Manager tenant URL.</p>
Devices Enrollment Mode	<p>Select the preferred device enrollment mode, which includes:</p> <ul style="list-style-type: none"> ■ Open Enrollment – Essentially allows anyone meeting the other enrollment criteria (authentication mode, restrictions, and so on) to enroll. Workspace ONE Direct Enrollment supports open enrollment. ■ Registered Devices Only – Only allowed users to enroll using devices you or they have registered. Device registration is the process of adding corporate devices to the UEM console before they are enrolled. For more information on registering devices, refer to the Enrollment section of the VMware Workspace ONE UEM Mobile Device Management Guide. Workspace ONE Direct Enrollment supports allowing only registered devices to enroll but only if registration tokens are not required.
Require Registration Token	<p>Visible only when Registered Devices Only is selected.</p> <p>If you restrict enrollment to registered devices only, you also have the option of requiring a registration token to be used for enrollment. This increases security by confirming that a particular user is authorized to enroll. You can send an email or SMS message with the enrollment token attached to users with Workspace ONE UEM accounts.</p>
Require Intelligent Hub Enrollment for iOS	Select this check box to require iOS device users to download and install the Workspace ONE Intelligent Hub before they can enroll. If disabled, Web Enrollment is available.
Require Intelligent Hub Enrollment for macOS	Select this check box to require macOS device users to download and install the Workspace ONE Intelligent Hub before they can enroll. If disabled, Web Enrollment is available.

Management Mode

Setting	Description
iOS	Enable iOS devices managed with Hub Services to enroll without being MDM managed.
Smart Groups	Enter smart groups that include devices that you do not want to manage with MDM.

Configure Hub Services to allow devices to enroll without MDM management.

Terms of Use Tab

Setting	Description
Require Enrollment Terms of Use Acceptance	Require that end users accept an end user license agreement (terms of service) at some point during the enrollment process. Terms of use is fully supported by Workspace ONE Direct Enrollment.
Add New Enrollment Terms of Use	Click this button to open the Terms of Use dialog, where you can quickly create a custom enrollment terms of use message. For more information on creating an enrollment terms of use, see the Terms of Use section of the VMware AirWatch Mobile Device Management Guide , available on docs.vmware.com.

Grouping Tab

Setting	Description
Group ID Assignment Mode	<p>Workspace ONE Direct Enrollment supports all assignment modes.</p> <ul style="list-style-type: none"> ■ Default - Select this option if users are provided with Group IDs for enrollment. The Group ID used determines what organization group the user is assigned to. ■ Prompt User to Select Group ID - Enable this option to allow directory service users to select a Group ID from a list upon enrollment. The Group ID Assignment section lists available organization groups and their associated Group IDs. This listing does not require you to perform group assignment mapping, but does mean users have the potential to select an incorrect Group ID. ■ Automatically Select Based on User Group - This option only applies if you are integrating with user groups. Enable this option to ensure that users are automatically assigned to organization groups based on their directory service group assignments. <p>The Group Assignment Settings section lists all the organization groups for the environment and their associated directory service user groups.</p> <p>Select the Edit Group Assignment button to modify the organization group/user group associations and set the rank of precedence each group has.</p> <p>For example, you have three groups, Executive, Sales, and Global, which are ranked in order of job role. Everyone is a member of Global, so if you were to rank that user group first, it puts all your users into a single organization group.</p> <p>Instead, if you rank Executives first, you ensure the small number of people belonging to that group are placed in their own organization group. Then rank Sales second, and you ensure that all Sales employees are placed in an organization group specific to sales. Rank Global last and anyone not already assigned to a group is placed in a separate organization group.</p>

Default

Setting	Description
Default Device Ownership	Select the default Device Ownership of devices enrollment into the current organization group. Workspace ONE Direct Enrollment supports setting a default device ownership.
Default Role	Select the default roles assigned to users at the current organization group, which can affect access to the Self-Service Portal. Workspace ONE Direct Enrollment supports setting a default role.
Default Action for Inactive Users	Select the default action that impacts Active Directory users if their devices become inactive. Workspace ONE Direct Enrollment supports setting a default action for inactive users.

User Group Sync

Setting	Description
Sync User Groups in Real Time for Workspace ONE	Workspace ONE can sync user groups for a given user as they register with the UEM console. Enabled by default, this feature is most effective when user groups are being used with great frequency for app assignment, profile assignment, policy assignment, or user mapping. This feature is CPU-intensive so unless your use case is similar to the above, disable this setting for improved performance and to prevent latency issues while launching the Workspace ONE application.

User Role Mapping

Setting	Description
Enable Directory Group-Based Mapping	Select this box to enable ranked assignments that link a directory user group to a specific Workspace ONE UEM role. Users belonging to a particular group are assigned the associated roles. If they belong to more than one group, they take the highest ranked pairing. You can edit the order in which role-infused user groups are ranked by selecting the Edit assignment button. Workspace ONE Direct Enrollment supports directory group-based mapping.

Restrictions Tab

Enrollment Restrictions

Setting	Description
User Access Control	<p>Workspace ONE Direct Enrollment supports all user access control options.</p> <p>Restrict Enrollment to Known Users – Enable to restrict enrollment only to users that exist in the UEM console. This restriction applies to directory users you manually added to the UEM console one by one or through batch import. It can also be used to lock down enrollment after an initial deployment that allowed anyone to enroll. This option enables you to be selective about who can enroll.</p> <p>You can allow all directory users who do not have accounts in the UEM console to enroll into Workspace ONE UEM by disabling this option. User accounts are automatically created during enrollment.</p> <p>Restrict Enrollment to Configured Groups – Enable to restrict enrollment and only allow users belonging to All Groups or Selected Groups (if you have integrated with user groups) to enroll devices. Do not select this option if you have not integrated with your directory services user groups.</p> <p>You can create Workspace ONE UEM user accounts during enrollment by disabling the option to allow all directory users to enroll. Select Enterprise Wipe devices of users that are removed from configured groups to automatically enterprise wipe devices. If All Groups is selected, devices not belonging to any user group are removed. If Selected Groups is selected, then devices not belonging to a particular user group are removed.</p> <p>One option for integrating with user groups is to create an "MDM Approved" directory service group and import it to Workspace ONE UEM. After this import step, you can add existing directory service user groups to the "MDM Approved" group as they become eligible for Workspace ONE UEM.</p>
Set limit for maximum enrolled devices at this OG and below	<p>Enable and Enter Device Limit to limit the number of devices allowed to enroll in the current organization group (OG).</p> <p>Workspace ONE Direct Enrollment supports this option.</p>

Policy Settings

- **Add Policy** – Click this button to add an enrollment restriction policy, which lets you define allowed ownership types, enrollment types, device limits, and more.

Setting	Description
Enrollment Restriction Policy Name	Enter a name for your enrollment restriction policy.
OrganizationGroup	Select an organization group from the drop-down menu. This is the OG to which your new enrollment restriction policy applies.
Policy Type	Select the type of enrollment restriction policy, which can be either Organization Group Default to apply to the selected organization group, or User Group Policy for specific User Groups through Group Assignment Settings on the Restrictions tab.
AllowedOwnership Types	<p>Select whether to permit or prevent Corporate - Dedicated, Corporate - Shared, and Employee Owned devices.</p> <p>Workspace ONE Direct Enrollment only supports the ownership types Corporate Dedicated and Employee Owned.</p>
AllowedEnrollment Types	Select whether to permit or prevent the enrollment of devices using MDM (Workspace ONE Intelligent Hub) and AirWatch Container (for iOS/Android) apps.

Setting	Description
Device Limit per User	<p>Select Unlimited to allow users to enroll as many devices as they want. Workspace ONE Direct Enrollment supports setting a device limit per user.</p> <p>Deselect this box to enter values for the Device Limit Per User section, to define the maximum number of devices per ownership type.</p> <ul style="list-style-type: none"> ■ Maximum Devices Per User ■ Corporate Max Devices ■ Shared Max Devices ■ Employee Owned Max Devices
Allowed DeviceTypes	<p>Select the Limit enrollment to specific platforms, models or operating systems check box to add additional device-specific restrictions.</p> <p>This option is supported by Workspace ONE Direct Enrollment.</p> <p>Note Current Microsoft functionality dictates that you cannot blacklist Windows Phone devices by IMEI or UDID.</p>
Device Level Restrictions Mode	<p>This option is only available if Limit enrollment to specific platforms, models or operating systems is selected in the Allowed Device Types option.</p> <p>Determine the kind of device limitations you should have.</p> <ul style="list-style-type: none"> ■ Only allow listed device types (Whitelist) – Select this option to explicitly allow only devices matching the parameters you enter and to block everything else. ■ Block listed device types (Blacklist) – Select this option to explicitly block devices matching the parameters you enter and to allow everything else. <p>For either device-level restrictions mode, select Add Device Restriction to choose a Platform, Model, Manufacturer (specific to Android devices), or Operating System. You may also add a Device Limit per defined device restriction. You may add multiple device restrictions.</p> <p>You can also block specific devices based on their IMEI, Serial Number or UDID by navigating to Devices > Lifecycle > Enrollment Status and selecting Add. This is an effective way to block a single device and prevent it from re-enrolling without affecting other users' devices. Preventing re-enrollment is also available as an option when performing an Enterprise Wipe.</p> <p>This option is supported by Workspace ONE Direct Enrollment.</p>

Management Requirements for Workspace ONE

Require MDM for Workspace ONE - Enable this feature and set the applicable devices to receive an MDM profile and to get managed when they enroll through Workspace ONE.

Group Assignment Settings

- **Edit Group Policies** – This button enables you to configure ranked assignments that link a directory user group to a specific Workspace ONE UEM enrollment restriction policy. Users belonging to a particular group must adhere to the associated restriction policy. If they belong to more than one group they will take the highest ranked pairing.

Optional Prompt Tab

The optional prompt settings let you configure various prompts that you set to display or not display during device enrollment. These optional prompts are web-based and are therefore cross-platform unless otherwise specified.

Setting	Description
Prompt for Device Ownership Type	<p>You can prompt the end user to select their device ownership type. Otherwise, configure a default device ownership type for the current organization group.</p> <p>Workspace ONE Direct Enrollment supports prompting for device ownership type.</p>
Display Welcome Message	<p>You can display a welcome message for your users early in the device enrollment process. You can configure both the header and the body of this welcome message by navigating to System > Localization > Localization Editor. Next, select the labels 'EnrollmentWelcomeMessageHeader' and 'EnrollmentWelcomeMessageBody' respectively.</p>
Display MDM Installation Message	<p>You can display a message for your users during the device enrollment process. You can configure both the header and the body of this MDM installation message by navigating to System > Localization > Localization Editor. Next, select the labels 'EnrollmentMdmInstallationMessageHeader' and 'EnrollmentMdmInstallationMessageBody' respectively.</p> <p>If you opt to customize your own header and body messages using the Localization Editor, you must opt to 'Override' in the Current Setting option. Doing so ensures that your customizations are used instead of the default messages.</p> <p>In addition to making one-off localization changes, you can also make localization changes in bulk by uploading an edited comma-separated values (CSV) file. Download this localization template CSV file by navigating to System > Localization > Localization Editor and select the Modify button. Edit the file per your preferences to affect bulk localization changes and upload it using the same screen.</p>
Enable Enrollment Email Prompt	<p>You can prompt the user to enter their email credentials during enrollment.</p> <p>The Enrollment Email Prompt requests the email address from the end user to populate that option in the user record automatically. This data is beneficial to organizations deploying email to devices using the {EmailAddress} lookup value.</p>
Enable Device Asset Number Prompt	<p>You can prompt the user to enter the device asset number during enrollment.</p> <p>Workspace ONE Direct Enrollment supports enrollment email prompts but only when Prompt for Device Ownership Type is enabled and only for Corporate Owned devices.</p>
Display Enrollment Transition Messages (Android Only)	<p>You can display or hide enrollment messages on Android devices.</p>
Enable TLS Mutual Auth for Windows	<p>You can force Windows Phone and Windows Devices to use endpoints secured by TLS Mutual Authentication which requires an extra setup and configuration. Contact Support for assistance.</p>

Customization Tab

Setting	Description
Use specific Message Template for each Platform	<p>Select this check box to use different enrollment message templates for the different platforms.</p> <p>This option is supported by Workspace ONE Direct Enrollment.</p>
Enrollment Support Email	<p>Enter the contact email for MDM support which will be displayed to users during enrollment.</p>
Enrollment Support Phone	<p>Enter the contact phone number for MDM support which will be displayed to users during enrollment.</p>

Setting	Description
Post-Enrollment Landing URL (iOS Only)	Enter the URL of the webpage you want end users redirected to after they enroll their devices. This field can be blank. This option is supported by Workspace ONE Direct Enrollment.
MDM Profile Message (iOS Only)	Enter the message you would like your users to see during the install MDM prompt. This field is optional and can be left blank. This option is supported by Workspace ONE Direct Enrollment.
Use Custom MDM Applications	Configure MDM Apps by adding them as managed applications and assigning them to MDM application groups. This option is supported by Workspace ONE Direct Enrollment.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / General / Friendly Name

The Friendly Name settings page lets you configure options related to device friendly names. The format you configure here is how devices will appear in the Workspace ONE UEM console.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Enable Custom Friendly Name	Select this check box to enable the configuration of a custom device friendly name string.
Device Friendly Name Format	Enter the friendly name format using the lookup values provided in the insert lookup value list by selecting the plus icon.
Set Device Name to Friendly Name	Check this box to automatically set the device's actual Device Name to match the Friendly Name format you configured. Applicable only to supervised devices with iOS 8 or greater.

Windows Rugged

Setting	Description
Use Registry Entry for Friendly Name (AirWatch 4.0 Hub Only)	Enable to use the Registry Entry instead of friendly names for devices using the Workspace ONE Intelligent Hub v4.0+ for Windows Rugged. You must enter quotes (") around the registry path for this option to work. For example, "HKEY_LOCAL_MACHINE\System\Device Info\Asset Number" or "HKLM\System\Device Info\Asset Number".

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / General / Lookup Fields

The **Lookup Fields** settings page lets on-premises customers create custom lookup fields from existing pre-created standard lookup fields. These lookup fields can then be used throughout the Workspace ONE UEM console.

For example, you can configure a custom lookup field that consists of a user's initials. In this example, you would choose 'User Email User Name' for the **Standard Lookup Field**, then give it a **Name** like 'Initials', choose 'Regex Lookup' for the **Custom Type** and in **Regular Expression**, enter the regular expression code that extracts the first letters of the first and last names of your users. Depending on what the 'User Email User Name' field looks like, it might be `(@"(\b[a-zA-Z])[a-zA-Z]* ?")`.

Upon a successful regex code expression with 'Return Result' selected, when you use the custom lookup field 'Initials,' in its place will be the user's initials: the first letter from their first name and the first letter from their last name.

All fields are required.

Setting	Description
Standard Lookup Field	Select from a list of pre-defined fields primarily used to identify either a user or a device.
Name	Enter the name of the customization.
Description	Enter a useful description of the customization to ease searching and record keeping.
Allow Inheritance	Allow your search to include inherited child organization groups.
Custom Type	Choose the mechanism of this customization, typically a regular expression (Regex).
Regular Expression	This field only appears when 'Regex' is chosen from the Custom Type field. A regular expression is a sequence of characters that forms a search pattern, mainly for use in pattern matching with strings, or string matching, i.e. "find and replace"-like operations.
On Match	Choose how the system should react when it discovers a match. Choose between Replace and Return Result . The regular expression in the custom lookup field is applied once per user. For this reason, there cannot be more than one result. Continuing the example cited above, when 'Return Result' is selected, the custom lookup value applies the regex to extract the user's initials and inserts these initials wherever the custom lookup value 'Initials' is used.
Replacement Value	This field only appears when 'Replace' is selected from the On Match field. The string entered here replaces the string discovered by the regular expression search. Continuing the example cited above, if you opt to 'Replace', the initials it extracts from the regex are outright replaced. In this case, the custom lookup value 'Initials' serves as a blanket replacement: whatever the regex finds, it is replaced with the value you enter here.

Devices & Users / General / Message Templates

The Message Templates settings page lets you create and manage message templates for use within other areas of the Workspace ONE UEM console.

You can create several types of message template, including those for enrollment, applications, compliance, and so on. Use the **Filters** feature to display only the message types you want to see.

- Select the **Add** button to display the **Add / Edit Message Template** screen.
- Select the name of the template in the **Name** column to view and edit the message template.
- With a radio button selected, click the **Copy** or **Delete** buttons to take that action on it.

Devices & Users / General / Notifications

The Notifications settings page enables you to utilize Lifecycle Notifications, which can be configured to supply enrollment and unenrollment confirmation emails.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

This optional setting can be configured by navigating to **Devices > Lifecycle > Settings > Notifications** and entering the following options for the following sections.

- **Device Unenrolled** - Send an email notification when a device unenrolls.
- **Device Enrolled Successfully** - Send an email notification when a device enrolls successfully.
- **Device Blocked by Enrollment Restriction** - Send an email notification if an enrollment restriction blocks a device. You can configure this behavior by navigating to **Groups & Settings > All Settings > Devices & Users > General > Enrollment** and selecting the **Restrictions** tab.

Setting	Description
Send Email To.	<ul style="list-style-type: none"> ■ None - Send no confirmation email upon a successful device block, enrollment, or unenrollment. ■ User - Send a confirmation email to the device user informing them of the successful device block, enrollment, or unenrollment. ■ CC - Send the same confirmation email to a single email address or multiple, comma-separated email addresses. ■ Message Template - Select the desired message template from the drop-down listing. You can add a new message template or edit an existing template by selecting the "Click here..." hyperlink that takes you to the Devices & Users > General > Message Templates settings page. ■ Administrator - Send a confirmation email to the Workspace ONE UEM administrator informing them of the successful device block, enrollment, or unenrollment. ■ To - Send the same confirmation email to a single email address or multiple, comma-separated email addresses.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / General / Privacy

The privacy settings page lets you define how device and user information are handled in the Workspace ONE UEM console. This is particularly useful in bring your own device (BYOD) deployments.

Data Types

For each ownership type (Corporate - Dedicated, Corporate - Shared, Employee Owned, and Unassigned) select whether to **Collect and Display** (in the Console), **Collect and Do Not Display**, or **Do Not Collect** for the listed data type.

These data types include the following.

- **GPS**
- **Telecom**
- **Applications**
- **Profiles**
- **Network**

Commands

For the remote commands you want administrators to be able to perform, select whether to **Allow**, **Allow With User Permission**, or **Prevent**. These commands are available for Android and/or Windows Phone devices. The asterisk beside the command denotes which device.

User Information

For **User Information**, select whether to **Display** or **Do Not Display** in the UEM console information for the data types presented. If a field is set to **Do Not Display**, then it displays as "Private" wherever it appears in the UEM console. This means you are not be able to search for fields you set to **Do Not Display**.

Do Not Disturb

Do Not Disturb Mode – **Enable** or **Disable** this mode.

Do Not Disturb (DND) provides a clean and automated way to halt profile, content, and application changes on enrolled devices for a set window of time directly from the UEM console. Integral MDM commands such as device wipe, enterprise wipe, and clear passcode still function when DND is enabled and the device is in DND mode.

DND mode is particularly useful for devices that are used or displayed in front of customers or guests. Admin messages, app updates and content changes may confuse end-users or disrupt demos and walkthroughs, so the ability to pause any changes allows uninterrupted usage. Once the Do Not Disturb period ends, all queued updates and commands are pushed down to the device automatically.

User Friendly Privacy Notice

Enable this option to display a user-friendly privacy notice to your end-users after they enroll a device.

Select to **Enable** or **Disable** the **User Friendly Privacy Notice** on the device.

When **Enabled**, you may choose **Yes** (display a privacy notice) or **No** (do not display a privacy notice) for each ownership level: **Employee Owned**, **Corporate - Dedicated**, **Corporate - Shared**, and **Unknown**. You must create a privacy notice before you assign ownership types to receive the notice.

Devices & Users / General / Shared Device

The Shared Device settings page lets you configure settings related to the shared device (multi-user) functionality of Workspace ONE UEM.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Grouping

Setting	Description
Group Assignment Mode	<p>Configure devices in one of three ways:</p> <ul style="list-style-type: none"> ■ Select Prompt User for Organization Group to have the end user enter a Group ID for an organization group upon login. <p>With this method, you have the flexibility to provide access to the settings, applications, and content of the organization group entered. Using this approach, an end user is not restricted to accessing only the settings, applications, and content for the organization group to which they are enrolled.</p> <ul style="list-style-type: none"> ■ Select Fixed Organization Group to limit your managed devices to settings and content applicable to a single organization group. <p>Each end user who logs in to a device has access to the same settings, applications, and content. This method can be beneficial in a retail use case where employees use shared devices for similar purposes such as checking inventory.</p> <ul style="list-style-type: none"> ■ Select User Group Organization Group to enable features based on both user groups and organization groups across your hierarchy. <p>When an end user logs in to a device, they have access to specific settings, applications, and content based on their assigned role within the hierarchy. For example, an end user is a member of the 'Sales' user group, and that user group is mapped to the 'Standard Access' organization group. When that end user logs in to the device, the device is configured with the settings, applications, and content available to the 'Standard Access' organization group.</p> <p>You can map user groups to organization groups on the UEM console. Navigate to Groups & Settings > All Settings > Devices & Users > General > Enrollment. Select the Grouping tab and fill in the required details.</p>
Always Prompt for Terms of Use	Prompts the end users to accept your Terms of Use agreement before they log in to a device.

Security

Setting	Description
Require Shared Device Passcode.	Require users to create a Shared Device passcode in the Self-Service Portal to check out devices. This passcode is different from a Single Sign On passcode or a device-level passcode.
Require Special Characters.	Require special characters in the shared device passcode, which includes characters such as @, %, &, and so forth.
Shared Device Passcode Minimum Length	Set the minimum character length of the shared passcode.
Shared Device Passcode Expiration Time (days)	Set the length of time (in days) the shared passcode expires.
Keep Shared device Passcode for minimum time (days)	Set the minimum amount of time (in days) the shared device passcode must be changed.
Passcode History	Set the number of passcodes that are remembered by the system, providing a more secure environment by preventing the user from reusing old passcodes.
Auto Log out Enabled	Configure an automatic log out after a specific time period.
Auto Log out After	Set the length of time that must elapse before the Auto Log out function activates in Minutes , Hours , or Days .
Enable Single App Mode.	<p>Select this check box to configure Single App Mode, which locks the device into a single application when an end user logs in to the device.</p> <p>To check out an iOS device in Single App Mode, end users log in using their credentials. When the device is checked in again, it returns to Single App Mode.</p> <p>Enabling Single App Mode also disables the Home button on the device.</p> <p>Note Single App Mode applies only to Supervised iOS devices.</p>
Clear Device Passcode on Logout (Android Only)	This setting controls whether the current device passcode is cleared when the user logs out (checks in) a multi-user shared device.
Clear App Data on Logout (Android Only)	Clear the app data when the user logs out of a shared device (checks it in).
Reinstall Apps on Logout (Android Work Managed Device and Android (Legacy) Only)	Use the drop-down to select whether to Always reinstall app between users or never reinstall app between users. For Android (Legacy) deployments, you can opt to reinstall app if the Hub cannot clear app data between users.

Logout Settings

Setting	Description
Clear Android App Data	This setting controls whether the application data from the current session is cleared when the user logs out of a shared device (checks it in).
Reinstall Android Apps	<p>If an app is assigned to the staging user and end-users logging in and out of the device, select one of the preferred app management behaviors: Always reinstall apps between users or Never reinstall apps between users.</p> <p>Warning: VMware recommends not enabling the Never option. When this option is set to Never, the software no longer requires that apps be deleted and reinstalled when one user stops using a shared device and another user begins using the same device. This means that the next user may have access to the original user's app data, including any personal or sensitive data.</p> <p>Ensuring the security of app data by end users using the same device is your sole responsibility. VMware is not liable for any damages in connection with your decision to enable this feature including direct, indirect, incidental, special, punitive, consequential damages or loss of profits, even if notice is given of the possibility of these kinds of damages.</p>
Clear Android Device Passcode	Enable to clear the Android device passcode, requiring the next user to create their own.
Clear iOS Device Passcode	Enable to clear the iOS device passcode, requiring the next user to create their own.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / General / Advanced

The Advanced settings page under Devices & Users lets you configure settings related to how the Workspace ONE™ UEM console identifies and reports device activity.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Device Inactivity Timeout	Enter the amount of time in minutes that a device not seen by the console will be identified as inactive.
Certificate Revocation Grace Period (hours)	<p>Enter the amount of time in hours after the discovery that a required certificate is missing from a device that the system shall wait before actually revoking the certificate.</p> <p>Given the vagaries of wireless technology and network bandwidth performance, this field is designed to prevent false negatives or times when a certificate is falsely identified as not existing on a device.</p>
Enrollment Session Timeout (min)	Enter the amount of time in minutes that the system will force an enrollment restart after a user's enrollment session begins without completing.

Setting	Description
Device Assignment Rules	Enables the use and assignment of IP address ranges as a grouping mechanism or device identifier.
Enable Auth Proxy Body Response	Legacy architecture designed to mimic the functionality of VMware Enterprise Systems Connector (VMware Enterprise Systems Connector) or EIS (Enterprise Integration Service).

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Android / Android EMM Registration

Android EMM Registration lets you configure the various options for integrating with Android. This page uses a wizard to help you set up the integration for devices. Enable these settings before beginning enrollment.

Configuration

The **Configuration** page shows Google Admin Console Settings and Google API settings after successful Android EMM registration.

Enrollment Settings

Setting	Description
Work Managed Enrollment Type (non-G suite only)	Choose if devices should be associated with the enrollment user or device. When using paid apps, User Based is preferred for optimal license allocation and most BYOD use cases. For scenarios where a single user will not be associated with the device (such as Kiosks), Device Based is preferred.
Fully-Managed Device Enrollments	Choose whether enrolled devices will use Work Managed Device or Corporate Owned Personally Enabled mode. <ul style="list-style-type: none"> ■ Work Managed Device is a fully-managed device that will be locked down providing employees with access to corporate apps only and no access to personal apps through the Google Play Store. ■ Corporate Owned Personally Enabled provides all the benefits of complete device management, but employees will receive a Work Profile to access corporate apps and will still have access to their personal Google Play Store outside of the Work Profile. This enrollment type is only available on Android 8.0+.

For more information on Android Device modes, see Understanding Android Device Modes available through docs.vmware.com.

Enrollment Restrictions

Setting	Description
Define the enrollment method for this Organization Group	Select whether to Always use Android , or Always Use Android (Legacy) , Define assignment group that use Android . If you select Define Assignment Group that use Android , all unassigned devices default to use Android (Legacy).
Assignment Groups	Select a smart group from the drop-down menu. When a smart group(s) is selected, devices or users that do not belong to that group(s) will go through Android legacy enrollment (device administrator). Devices that belong to smart group will enroll in Work Profile or Work Managed assuming they support these enrollment modes For more information on Smart Groups, see Smart Groups Overview in the Mobile Device Management (MDM) documentation.

Devices & Users / Android / Hub Settings

The Android Hub Settings page lets you configure various options that affect the Android Hub mobile app. Adjusting these intervals can impact battery life, with smaller values equating to more frequent pings and greater power consumption.

To access the Workspace ONE Intelligent Hub Settings navigate to **Groups & Settings > All Settings > Devices & Users > Android > Hub Settings**.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

General

Setting	Descriptions
Heartbeat Interval (min)	Enter the heartbeat time interval, which is how frequently the Workspace ONE Intelligent Hub checks in with the Workspace ONE UEM server. Reports beacon data to the Workspace ONE UEM console. The primary purpose of this report is to show compromised device status. However, beacon data also includes GPS, IP address and other minor data, such as model and OS version.
Data Sample Interval (min)	Enter the data sample time interval, which is how frequently the Workspace ONE Intelligent Hub collects data from the device. Collects interrogator data and reports all data collected by the Workspace ONE Intelligent Hub, including Telecom and Network data, as well as the battery, power and memory status.
Data Transmit Interval (min)	Enter the data transmit time interval, which is how frequently the Workspace ONE Intelligent Hub sends data to the Workspace ONE UEM server. Reports interrogator data to the Workspace ONE UEM console. This value should always be greater than the Data Sample Interval value.
Profile Refresh Interval (min)	Enter the profile refresh time interval, which is how frequently the device profile list for the device is refreshed on the Workspace ONE UEM server. Checks in with the Workspace ONE UEM console for profile updates or new profiles.
Require Google Account	Require a Google Account to leverage Google Cloud Messaging (GCM) to send remote commands to devices. Only deselect this option if you are utilizing AWCm.
Require Phone Number	Enable an additional prompt during enrollment. This phone number is recorded in Workspace ONE UEM to serve as a backup contact number in case devices are lost, turned off or do not have access to Internet.

Setting	Descriptions
Block User Unenrollment	Select this option to ensure end users cannot unenroll their devices by disabling the 'Unenroll' option in the Workspace ONE Intelligent Hub menu. On Samsung devices using Android Legacy, this will also prevent Device Administrator deactivation for the Workspace ONE Intelligent Hub.
Device Services Version	Displays OEM service version.

Application List

The Application List detects specific, blacklisted apps that are installed on a device, or detect all apps that are not whitelisted. You can either specifically prohibit certain apps, such as social media or entertainment apps, or specifically permit only the apps you specify, such as internal applications for business use.

Setting	Description
Application List Interval (min)	Enter the frequency at which the Workspace ONE Intelligent Hub checks the application list.

Applications

Setting	Description
Install Options	Select how end users will be prompted to install new internal applications. You can provide a Direct Prompt , a Status Bar Notification , or opt to have No Notification .
SafetyNet App Verification	Enable to allow app verification which scans apps installed on the device before they are downloaded to detect potentially harmful apps.

Samsung Knox

For more information about these settings or Samsung Knox in general, refer to the **VMware AirWatch Containerization with Samsung Knox Guide**.

Setting	Description
Enable Containers	Select Enabled to allow profile creation for Samsung Knox Containers for Android (Legacy enrollment) and to allow the Android Hub to create application containers for Samsung Knox devices. If Android EMM registration has been completed, enabling containers will activate Knox Play for Work configuration on Samsung devices.
Knox License Key	Enter your Samsung Knox License Key. You can enter a Knox License Key without enabling Knox containers (which applies to Android (Legacy)).
Enable Audit Logging	Select Enabled to turn on audit logging and the related settings below. The Workspace ONE UEM console has the ability to monitor errors that might prevent successful creation of the Knox container. The log provides the cause of the error and what needs to be resolved for successful Knox deployment. The audit logs are sent to the UEM console from the Knox enabled devices and stored in the Device Details page. The Transmits Logs Automatically setting determines the threshold at which the log file is reported to the device details.

Setting	Description
Logging Level	<p>Determines how severe an error has to be in order for it to be sent to the log file. The logging levels are listed in order of severity where notice is the least severe and alert is the highest.</p> <ul style="list-style-type: none"> ■ Alert ■ Critical ■ Error ■ Warning ■ Notice
Critical Log Size	Enter a percentage (up to 70 percent) to define the critical log size. When the log file passes this percentage, a critical log size alert is sent to the admin.
Maximum Log Size	Enter a percentage (up to 90 percent) to define the maximum log size. When the log file passes this percentage, a maximum log size alert is sent to the admin.
Full Log size	Set to 97 percent by default. When the log file reaches this percentage, a full log size alert is sent to the admin and immediate action is required.
Transmits Logs Automatically	<p>Determines when the audit logs are to be transmitted to the console to notify the admins of errors.</p> <ul style="list-style-type: none"> ■ Never – The log file will never be sent transmitted to the console. ■ Critical – The log file needs be at critical size to be transmitted to the console. ■ Maximum – The log file needs be at maximum size to be transmitted to the console. ■ Full – The log file needs be at full size to be transmitted to the console.

Location

Setting	Descriptions
Heartbeat Interval (min)	Enter the heartbeat time interval, which is how frequently the Workspace ONE Intelligent Hub checks in with the Workspace ONE UEM server. Reports beacon data to the Workspace ONE UEM console. The primary purpose of this report is to show compromised device status. However, beacon data also includes GPS, IP address and other minor data, such as model and OS version.
Data Sample Interval (min)	Enter the data sample time interval, which is how frequently the Workspace ONE Intelligent Hub collects data from the device. Collects interrogator data and reports all data collected by the Workspace ONE Intelligent Hub, including Telecom and Network data, as well as the battery, power and memory status.
Data Transmit Interval (min)	Enter the data transmit time interval, which is how frequently the Workspace ONE Intelligent Hub sends data to the Workspace ONE UEM server. Reports interrogator data to the Workspace ONE UEM console. This value should always be greater than the Data Sample Interval value.
Profile Refresh Interval (min)	Enter the profile refresh time interval, which is how frequently the device profile list for the device is refreshed on the Workspace ONE UEM server. Checks in with the Workspace ONE UEM console for profile updates or new profiles.
Require Google Account	Require a Google Account to leverage Google Cloud Messaging (GCM) to send remote commands to devices. Only deselect this option if you are utilizing AWCM.
Require Phone Number	Enable an additional prompt during enrollment. This phone number is recorded in Workspace ONE UEM to serve as a backup contact number in case devices are lost, turned off or do not have access to Internet.

Setting	Descriptions
Block User Unenrollment	Select this option to ensure end users cannot unenroll their devices by disabling the 'Unenroll' option in the Workspace ONE Intelligent Hub menu. On Samsung devices using Android Legacy, this will also prevent Device Administrator deactivation for the Workspace ONE Intelligent Hub.
Device Services Version	Displays OEM service version.

Telecom

Enable specific Telecom settings like Call Logs, SMS Logs and Cellular Data Usage to allow logging and tracking of device use.

Setting	Description
Enable Call Logs	Collects information from incoming and outgoing phone calls made devices registered with Workspace ONE UEM.
Enable SMS Logs	Reports that log any incoming and outgoing SMS messages to devices.
Enable Cellular Data Usage	Allows the Workspace ONE UEM console to create reports which details data usage.

Suspicious Activity Logs

When Suspicious Activity Log settings are enabled, devices will log every Bluetooth and USB connection that occurs except Bluetooth headsets and USB charging. To access Suspicious Activity Logs, Syslog settings must be correctly configured. For more information on Syslog configuration, see [System / Enterprise Integration / Syslog](#)

Setting	Description
Bluetooth Connections	Logs all bluetooth connections made except for Bluetooth headsets.
USB Connections	Logs all USB connections made except for USB charging ad USB headsets.

You must also enable Privacy and Location settings under **Devices & Users > General > Privacy** under the GPS section.

AirWatch Cloud Messaging

AirWatch Cloud Messaging (AWCM) provides an internal communication solution for the entire Workspace ONE UEM solution as a comprehensive replacement for Google Cloud Messaging (GCM).

Setting	Description
Use AWCM Instead of C2DM As Push Notification Service	Set to Enabled to enable AWCM.
AWCM Client Deployment Type.	Set to Always Running if you want the system and device have a constant and ongoing line of communication.
AWCM Client Timeout Value (Mins)	Determines how much idle time can pass before the client responds to the AWCM server.

Remote Management

Remote Management allows you to directly control a device for troubleshooting or to ensure a device is properly provisioned.

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	<p>Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin.</p> <ul style="list-style-type: none"> ■ Enter a Seek Permission Message that the end user sees when a remote request is sent. ■ Enter the Yes Caption message for the accept button the end user sees on the Seek Permission request. ■ Enter the No Caption message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	<p>Enter the port used to communicate between the Remote Management Hub and the Tunnel Agent on the end-user device.</p> <p>This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.</p>
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

Product Provisioning

- **Job Log Level** – A job occurs whenever files/actions are performed as part of product provisioning. With this setting, you can set the level of the job log level to meet your organization's logging level needs.

SDK Profile

Enterprises can integrate any existing company specific apps with the use of an AirWatch Software Development Kit (SDK). Select which SDK profile to deploy to your devices by using the SDK Profile V2 option in the Workspace ONE Intelligent Hub settings.

- **SDK Profile V2** – Select the profile that will provide the Workspace ONE Intelligent Hub with the SDK settings configured for that organization group.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Android / Google Play Integration

For on-premises customers, Workspace ONE UEM has updated the logic for how to search for public Android applications from the Google Play Store for the purpose of deploying applications. To enable this functionality, enter placeholder data (for example, "AcmeUser", "AcmePassword", "AcmeID") in the fields on the Google Play Integration settings page.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Google account username	Enter a placeholder Google Account user name.
Google account password	Enter a placeholder Google Account password.
Android Device ID	Enter a placeholder Android Device ID to provide the system with access to all applications in the Google Play Store.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Android / Auto-Enrollment

The **Auto-Enrollment** settings page is used to enable automatic enrollment for Android devices. Auto enrollment is only available for Intel devices that are a part of the Intel World's Ahead Program. Currently,

no other OEM supports this process. Refer to the Android Device Enrollment section of the Android Platform Guide for information on enrolling all other devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Enable Auto-Enrollment	Select Enabled to turn on auto-enrollment features for devices.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Android / Service Applications

Service Applications are apps downloaded in conjunction with the Workspace ONE Intelligent Hub depending on a certain functionality needed by the customer. The two service apps deployed are the 'AirWatch Launcher' and 'Telecom Sampler'. This section will detail how to deploy these settings.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

To access the Service Application settings navigate to: **Groups & Settings > All Settings > Devices & Users > Android > Service Applications**.

Setting	Description
Require Service App	Select to ensure end users get the Service App.
Push Service App from Play Store	Select to install the OEM service through the Google Play Store before or during enrollment. Pushing the Service App simplifies enrollment for your end users by removing the need to accept "unknown sources" during the enrollment process.
Download Folder	Provide a location for the file download. This option only appears if Push Service App from Play Store is disabled.
Always use the Latest Version of Telecom Sampler	Select to use latest or de-select to choose a specific Telecom Sampler Version .
Telecom Sampler Version	Select the desired Telecom Sampler version.

Setting	Description
Always use the Latest Version of AirWatch Launcher	Select to use latest or de-select to choose a specific AirWatch Launcher Version .
AirWatch Launcher Version	Select the desired Launcher version.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Android / Security

The Security page adds additional security settings for Android devices to protect sensitive data from unauthorized access to the device database. As part of the enrollment process, end users will create a passphrase code, which generates a key used to access the device database. When Key Encryption With User Input is enabled on the Security page and someone tries to access the database without that passphrase, access is denied. To enable this feature, Single Sign On must be enabled through the AirWatch SDK.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

The passphrase requirements can be set to allow the end user to only enter the passphrase during enrollment for a one-time prompt by enabling **Allow Remember Authentication**.

Important If you enable Allow Remember Authentication, this stores the user key on the device but renders the sensitive data vulnerable to unauthorized access.

Note In order for the Workspace ONE Intelligent Hub for Android to share an application passcode or SSO session with other SDK apps, you must enable **Key Encryption with User Input**.

Setting	Description
Key Encryption with User Input	Allows the Workspace ONE Intelligent Hub to encrypt the sensitive data with a user-derived key. Enable this only when required.
Allow Remember Authentication	Enable to save the user-derived key on the device so it does not need to be entered each time.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Android / Samsung Enterprise FOTA

Samsung Enterprise Firmware Over the Air (EFOTA) allows you to manage and restrict firmware updates on Samsung devices running Android 7.0 Nougat and higher. Use this page to enter your EFOTA settings provided by your licensed reseller. After saving these settings, use the Android restrictions profile to push lock down devices to their current firmware version, and view and manage available updates from the Updates page in the Workspace ONE UEM console.

Note Samsung EFOTA can only be configured at customer level Organization Group so all devices registered under that Organization Group receive updates. Consider creating a separate Organization Group for testing before pushing to all devices.

Setting	Description
Customer ID	Enter the ID provided by your licensed reseller.
License	Enter the license provided by your licensed reseller.
Client ID	Enter the Client ID provided by your licensed reseller.
Client Secret	Enter the Client Secret provided by your licensed reseller.

Devices & Users / Apple / APNs for MDM

The APNs for MDM settings page lets you generate or upload your Apple Push Notification service (APNs) certificate, which is required to manage Apple devices. If you do not already have an APNs certificate, you can generate a new one on this page. If you do have such a certificate, you can upload it here.

For more information, please see the *APNs for Applications Renewal Script Notification* KB article: <https://support.workspaceone.com/articles/360010936073>.

Devices & Users / Apple / Apple iOS / APNs for Applications

The APNs for Applications page displays the APNs certificates that correspond to Workspace ONE UEM apps on the app store. These are required for sending push notifications to apps, and in most cases these are settings you should not alter unless instructed.

For more information, please see the *APNs for Applications Renewal Script Notification* KB article: <https://support.workspaceone.com/articles/360010936073>.

Devices & Users / Apple / Apple iOS / Hub Settings

The iOS Hub Settings page lets you configure various options that affect the iOS Hub mobile app.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

General Tab

Setting	Description
General	
Disable Un-Enroll in Hub	This setting disables the user's ability to unenroll from Workspace ONE UEM MDM using the Workspace ONE Intelligent Hub. This setting is only available in the Workspace ONE Intelligent Hub v4.9.2 and higher.
Background App Refresh	<p>This setting tells the Workspace ONE Intelligent Hub the maximum allowed time interval to refresh app content. Some applications run for a brief period before reaching a suspended state. Background App Refresh is a feature in iOS where the application itself wakes from this suspended state. During this refresh, the Workspace ONE Intelligent Hub reports information, such as compromised detection, hardware details, GPS, iBeacon, and telecom, to the UEM console. The frequency at which the Workspace ONE Intelligent Hub refreshes is controlled by the OS and only completed during efficient times, such as when the device is plugged into a power source, frequency of use, or connected to Wi-Fi.</p> <p>To take advantage of the Background App Refresh feature, this setting must be enabled in the UEM console, the Workspace ONE Intelligent Hub cannot be killed on the device, and Background App Refresh must be enabled on the device for the Workspace ONE Intelligent Hub under Settings > General > Background App Refresh.</p>
Minimum Refresh Interval	Select the minimum amount of time that must pass before the device attempts to refresh app content.
Transmit on Wi-Fi only	Enable background refresh to occur over Wi-Fi connections only.
Area	
Collect Location Data	This setting enables the Workspace ONE Intelligent Hub to collect GPS data from devices. Whether or not data is actually collected depends on the privacy settings set in Devices > Device Settings > General > Privacy .
Detect iBeacon Region	This setting enables the Workspace ONE Intelligent Hub to listen to iBeacon information in regions where the device is located.
Telecom	
Collect Cellular Data Usage	This setting enables the Workspace ONE Intelligent Hub to collect cellular data use from devices. Whether or not data is actually collected depends on the privacy settings set in Devices > Device Settings > General > Privacy .
Self Service Setting	
Self Service Enabled	<p>This setting allows users to view their user account status, device compliance status, and assigned compliance policies from within the Workspace ONE Intelligent Hub. If enabled, users can see if their devices are compliant.</p> <p>For more information about enabling users to sync their devices to check for compliance status, see the following Workspace ONE UEM Knowledge Base article: https://support.air-watch.com/articles/115001662408.</p>
SDK Profile	
SDK Profile (Legacy)	This setting specifies the SDK profile you want to apply to the Workspace ONE Intelligent Hub. SDK profiles can be used to enforce geofencing, create custom branding for the Workspace ONE Intelligent Hub and more.
SDK Profile V2	This setting specifies the SDK V2 profile you want to apply to the Workspace ONE Intelligent Hub. SDK profiles can be used to enforce geofencing, create custom branding for the Workspace ONE Intelligent Hub and more.

Notification Tab

These notification settings ensure the Workspace ONE Intelligent Hub can send push notifications.

Notification (iOS Only)

Use this tab to configure notifications that are sent to devices from the UEM console.

Setting	Description
Application Type	Choose to configure the Workspace ONE Intelligent Hub either as a system app or an internal Workspace ONE UEM app to set system preferences. By default, the application type is set as System.
Application Name	Select an internal application from the drop-down menu. Ensure the Application Name appears the same way as it is does on the Internal List View page on the Apps & Books tab in the UEM console. Only internal applications with APNs certificates that were uploaded at the time the application was uploaded to the Console are seen here.
Bundle ID	This field is populated based on the selections above. This Bundle ID matches the application bundle ID that has been uploaded internally or selected from the drop-down menu.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Apple iOS / Managed Settings

The iOS Managed Settings page lets you configure a few additional settings related to the Workspace ONE Intelligent Hub and managing iOS devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Default Managed Settings

Setting	Description
Apply Default Settings To	Select which ownership types you want each of the default managed settings below to apply to.
Voice Roaming	Select the checkbox to allow voice roaming.
Data Roaming	Select the checkbox to allow data roaming.
Personal Hotspot	Select the checkbox to allow personal hotspot functionality.
Activation Lock	Select the checkbox to allow activation lock functionality.

Default Wallpaper

Setting	Description
Apply Default Settings To	Select the ownership type(s) to which the following default managed settings are applied.
Lock Screen Image	Upload a lock screen image that displays when an end user locks their device.
Home Screen Image	Upload the home screen image that displays on the device.

Organization Information

Send notifications or other MDM prompts with customized organization information.

Setting	Description
Organization Name	Enter the name of the organization.
Organization Phone Number	Enter the organization phone number.
Organization Email	Enter the organization email address.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Apple macOS / Hub Application

The macOS Hub Application settings page lets you configure various options that affect the macOS Hub application.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Fully Qualified Path on local server to the Workspace ONE Intelligent Hub files for MAC devices	This is the default location where the Workspace ONE Intelligent Hub is stored on the local server. Only change this if needed. If the file path is incorrectly defined, end users cannot download the Workspace ONE Intelligent Hub post-enrollment.
Download Mac Hub Post Enrollment	Select this checkbox to allow the Workspace ONE Intelligent Hub to be downloaded post-enrollment by side-loading or from a web browser.
Download Hub	Use this button to download the latest version of the Workspace ONE Intelligent Hub from the server.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Apple macOS / Hub Settings

The macOS Hub Settings page lets you configure various options that affect the macOS Hub application. Use these settings to determine how often to collect data from devices, to allow passcode enforcement through Hub message prompts, to allow AirWatch Cloud Messaging so that devices receive push notifications and information about updates when available, and to choose how and when to allow updates.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
General	
Download Latest Version	Download the latest version of the VMware Workspace ONE Intelligent Hub.
Install Hub after Enrollment	Enable or disable the option to automatically install the Hub on devices after enrollment through Apple Business Manager's DEP or Web enrollment.
Check-in Interval	Enter the frequency for the Hub to check in with the server to receive new commands.
Data Sample Interval	Enter the frequency for the Hub to scan devices to collect data such as product provisioning status, disk encryption status, custom attributes, GPS location, and other basic system information.
Data Transmit Interval	Enter the frequency for the Hub to send data samples to the Hub UEM server.
Uninstall Privileges	Enable or disable the option to provide end users the ability to uninstall the Hub application from their devices.
Security	
Enforce Password	Enable the option to prompt end users to create a new password that meets MDM profile requirements. If disabled, the end users are only prompted when logging out and logging back in.
Privacy	
Request to collect Location Data	Enable or disable the option to prompt end users to allow the collection of GPS location data.

Setting	Description
AirWatch Cloud Messaging	
Use AWCM	Enable the option for the AirWatch Cloud Messaging (AWCM) service to allow the real-time communication between the server and the Hub. If disabled, the Hub will not receive any commands and samples until the next scheduled interval check-in.
Intelligent Hub Updates	
Automatic Updates	Enable the option for the Hub to automatically check to see if updates are available. If disabled, the end users must manually check for updates within the Hub.
Upgrade Silently	Enable the option for the upgrades to automatically install in the background without prompting the end users. If disabled, the end users are prompted to upgrade when new updates are available.
Remote Management	
Request Permission	<p>Enable the option to prompt end users asking for permission to establish remote management connections with their devices. When you enable this setting, following options appear.</p> <ul style="list-style-type: none"> ■ Enter a Seek Permission Message that the end user can see when a remote request is sent. ■ Enter the Yes Caption message for the accept button that the end user can see on the Seek Permission request. ■ Enter the No Caption message for the decline button that the end user can see on the Seek Permission request.
Remote Management Port	Enter the port number used by the device remote management application to listen to the remote management connections.
Max Sessions	Enter the maximum number of concurrent remote management sessions that can be opened on the devices.
Number of Retries	Enter the maximum number of times the devices try to establish connections with the Tunnel server.
Retry Frequency (seconds)	Enter the interval between retries to establish connections with the Tunnel server.
Heartbeat Interval (seconds)	Enter the interval to send heartbeat samples from the Tunnel server to the devices.
Connection Lost Retry Frequency (seconds)	Enter the interval to check for the network connectivity availability.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Apple macOS / Software Management

Use the macOS Software Distribution method to initiate the software management lifecycle for macOS applications.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Enable **Software Management**. At this point, make sure that you verify if the **File Storage** is enabled. If there is no file storage enabled, you are requested to enable it.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / AppleCare

Use the Apple Care settings page to manage options related to Workspace ONE UEM integration with AppleCare.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Action
GSX User ID	Enter the account user ID.
GSX Password	Enter the account password.
Sold-to Account Number	Enter the 10-digit service account number. This account number can be found in the GSX portal at the bottom of the web page.
Time Zone	Use the drop-down menu to select the appropriate time zone.
Language	Use the drop-down menu to choose a language.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Automated Enrollment

The Automated Enrollment settings page lets you create and export an MDM profile that you can then import into Apple Configurator when staging devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Enable Automated Enrollment	Select this check box to display the staging settings you can configure.
Platform	Select which Apple platform this profile will be used for.

Setting	Description
Staging Mode	<p>Select the appropriate Staging Mode depending on how the device is going to be used and how the device must enroll. You can choose to pre-register devices and enroll using Apple Configurator. By pre-registering devices and selecting the None or Single User mode, you can pre-assign the end user for each device. However, you cannot pre-register Multi User devices.</p> <ul style="list-style-type: none"> ■ None – Does not stage device for other users. For non-registered devices, all devices will be enrolled under the Default Enrollment User. In this case, only non-staging users are available as default staging user options. <p>Important If you do not pre-register your devices and select None and specify a default enrollment user, then all devices that receive the .mobileconfig file will be enrolled to that user. To ensure devices are enrolled to distinct users, pre-register them to specific users or create a staging user account and select Single User as your Staging Mode.</p> <ul style="list-style-type: none"> ■ Single User – Stages device for a single, known or unknown user. Only staging users are available as Default Enrollment User options. When end users open the Workspace ONE Intelligent Hub, they must enter credentials to fully enroll the staged device. At that time, the device details will update in the UEM console and the device is associated with that end user. ■ Multi User – Places device into Shared Device Mode. This stages the device for multiple, known or unknown users. Only staging users are available as Default Enrollment User options. When end users open the Workspace ONE Intelligent Hub, they must enter credentials to check out the device for use.
Default Staging User	Set a Default Staging user if you are using either the None or Single User staging modes.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / MDM Sample Schedule

The Apple MDM Sample Schedule settings page lets you configure the time intervals at which certain data samples from Apple devices are sent to the UEM console server.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. **Inherit** means use the settings of the current organization group's parent OG, while **Override** enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Device Information Sample	Enter the frequency by which device information is refreshed on the Workspace ONE UEM server.
Application List Sample	Enter the frequency by which the application list is refreshed on the Workspace ONE UEM server.
Certificate List Sample	Enter the frequency by which the certificate list is refreshed on the Workspace ONE UEM server.
Profile List Sample	Enter the frequency by which the profile list is refreshed on the server.
Provisioning Profile List Sample	Enter the frequency by which the provisioning profile list is refreshed on the server. (iOS only)
Restriction List Sample	Enter the frequency by which the restrictions list is refreshed on the server. (iOS only)

Setting	Description
Security Information Sample	Enter the frequency by which the security information is refreshed on the server.
Managed App List Sample	the frequency by which the managed app list is refreshed on the server. (iOS only)
Sample	Enter the frequency by which the scheduler determines how often a silent APNs is sent to the device to poll for compromised detection, data usage, and GPS, if these Hub settings are enabled for the device. This requires the Workspace ONE Intelligent Hub 4.9 or higher and is only for iOS 7 or higher devices. (Reference macOS Hub Settings for information on macOS scheduling.)
Non-Compliant Device Sample	Enter the frequency by which Workspace ONE UEM queries non-compliant devices, to decrease the delay between when an end user takes actions to make their device compliant and when Workspace ONE UEM detects that action.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Device Enrollment Program

The Device Enrollment Program settings page lets you configure DEP-based enrollment within Workspace ONE UEM. DEP settings can be configured at any Organization Group. A wizard displays when you initially configure the DEP Profile, which walks you through the setup process.

The specific steps are not mentioned here because they are included as part of a separate guide.

Devices & Users / Apple / Profiles

The Apple profile page allows you to define security profile properties for your MDM profiles. You can optionally select to sign and encrypt profiles here. You can configure these settings during your initial set-up.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Encrypt Profiles	Select this checkbox to encrypt all MDM and device profiles that are installed on the devices.
Sign Profiles (Requires Server SSL Certificate)	Select this checkbox to sign MDM and device profiles with a SSL certificate that is used to establish trust with the device services server.

Setting	Description
Prompt devices to update MDM profile for iOS 5 Permissions	This is a legacy setting used to provide compatibility with iOS 5. This checkbox does not need to be selected unless you are working with an iOS 5 device.
Signing Certificate	Use the Upload button to upload a third-party SSL certificate to sign the profile. The SSL certificate should be the same one used on the device services end point.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / SCEP

Use this page to configure settings for SCEP certificate enrollment on iOS devices. Select SCEP settings to retrieve a SCEP certificate instead of a self-signed enrollment certificate.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Use in Enrollment	Select this checkbox to retrieve a SCEP certificate during enrollment instead of a regular enrollment certificate.
SCEP Certificate Authority	Select the certificate. If one is not available, go to Groups and Settings > All settings > System > Enterprise Integration > Certificate Authorities and follow the prompts to add a certificate.
SCEP Certificate Template	Select the certificate template. If one is not available, go to Groups and Settings > All settings > System > Enterprise Integration > Certificate Authorities > Request Templates and follow the prompts to add a certificate template.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Apple / Install Fonts

With the iOS Install Fonts settings, you can add fonts that you want to install on device. Available to macOS Yosemite and devices running iOS 7 and higher, the UEM console provides a means to upload fonts and install them onto devices. Installing specific fonts allows users to view and read text that is not supported by standard means.

Compatible font file types include .ttf or .otf. There is no limit to the number of fonts you are can install on devices and you can remove a font at any time.

Drag a supported font file type (.ttf or .otf) onto the screen and select **Save**.

Devices & Users / Apple / Education

The Apple Education page can be used to enable Apple Education functionality, which then allows for integration with Apple School Manager.

Note This functionality is only available to those with Workspace ONE UEM administrator roles and above.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	General
Enable Education Features	Select Enable to turn education functionality on.
Class Source	Select your Apple or Workspace ONE UEM as your Education functionality provider. Note that changing sources and saving the configuration will delete all existing classes.
Set Maximum Resident Users	Specify the maximum number of users each device's memory can support. This value divides the local storage on the iPad evenly for that number of users. If the number of users exceeds this setting, additional users' information is stored on iCloud instead of on the device.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Blackberry / Blackberry 10 / General

Specify your company's PowerShell information so that the Workspace ONE UEM console can use PowerShell commands to push profiles using the Exchange ActiveSync protocol.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
PowerShell URL	Specify the URL where the UEM console can access your PowerShell service.
Username	Specify the username that UEM console needs to communicate with the PowerShell service.
Password	Specify the password for the user account.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Blackberry / Blackberry 10 / Hub Settings

The Blackberry 10 Hub Settings page lets you configure various options related to the Blackberry 10 Hub.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Heartbeat Interval (min)	Enter the time interval by which the Workspace ONE Intelligent Hub will check in with the Workspace ONE UEM server.
Data Sample Interval (min)	Enter the time interval by which the Workspace ONE Intelligent Hub will collect data from the device.
Profile Refresh Interval (min)	Enter the time interval by which the device profile list is refreshed on the Workspace ONE UEM server.
Administrative Passcode	Enter the passcode that is required to access the Workspace ONE Intelligent Hub settings on the device.
Enable GPS	Select whether to enable the Workspace ONE Intelligent Hub to collect GPS coordinates of the device.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Blackberry / Blackberry 10 / BES 10 Settings

The Blackberry 10 BES Settings page lets you configure options related to your BES 10 component. For more information about integrating with your BES, refer to the BES 10 Server Integration section in the **VMware AirWatch BlackBerry Platform Guide**, available on docs.vmware.com.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
BES URL	Enter the URL for the BlackBerry Web Services that contains all the web service APIs used to synchronize the Workspace ONE UEM solution and the BES 10 server. The URL format is <code>https://<BES_URL>:38443</code> .
BES Admin Username / Password	Enter the username and password needed to authenticate with the BES 10 server in the BES Admin Username field and the BES Admin Password field.
Authentication Method	Ensure that the Authentication Method field is set to Active Directory or BlackBerry Administration Service .
Domain	Enter a domain for the BES 10 server in the Domain field.

Setting	Description
Ignore SSL Errors	If you want to ignore Secure Socket Layer (SSL) certificate errors between Workspace ONE UEM component and the BES 10 server then select the Ignore SSL Errors checkbox.
BES Sync Batch Size	Enter a value in the BES Sync Batch Size field for the maximum size of the message to be sent from the BES 10 server through the Workspace ONE UEM console to the device.
Activation Code Expiration	Enter the number of hours in the Activation Code Expiration field for the amount of time the end user has to activate their BES 10 server.
Message Type	Select either the Email or SMS radio button to determine the method used to deliver the BES Registration Message .
BES Registration Message	Select from the BES Registration Message drop-down a message the end user receives upon registration.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Blackberry / Legacy Blackberry / Hub Settings

The Legacy Blackberry Hub settings page lets you configure options related to the legacy Blackberry Hub.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Heartbeat Interval	Set the time (in minutes) the Workspace ONE Intelligent Hub waits before checking in with the Workspace ONE UEM console.
Data Sample Interval	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to collect data from the device.
Profile Refresh Interval	Set the frequency (in minutes) the profile list of each device will be refreshed on the server.
Collect Location Data	Set the Workspace ONE Intelligent Hub to send GPS data to the UEM console.
GPS Sample Interval	Set the interval at which the Workspace ONE Intelligent Hub collects sample GPS data for the device.

Setting	Description
Administrative Passcode	Set the passcode needed to access the Settings area of the Workspace ONE Intelligent Hub.
Enable Branding	Brand the Workspace ONE Intelligent Hub with attributes specific to your company. Set the following applicable options: <ul style="list-style-type: none"> ■ Login Title Text – Specify the text users view to log in to the Workspace ONE Intelligent Hub. ■ Toolbar – Specify the color of the toolbar in the Workspace ONE Intelligent Hub. ■ Background – Specify the background color of the Workspace ONE Intelligent Hub. ■ Background Image – Set a specific image for the background of the Workspace ONE Intelligent Hub. ■ Company Logo – Import your company logo in to the Workspace ONE Intelligent Hub.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / BlackBerry / Legacy BlackBerry / BES Settings

The Legacy Blackberry BES Settings page lets you configure options related to your BES component. For more information about integrating with your BES, refer to the BES 10 Server Integration section in the **BlackBerry Platform Guide**, available on docs.vmware.com.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
BWS URL	Enter the URL for the BlackBerry Web Services that contains all the web service APIs used to synchronize the Workspace ONE UEM solution and the BES. The URL format is https://<BES_URL>/enterprise/admin/ws.
BWS Util URL	Enter the URL for the BlackBerry Web Services Utility that contains helper APIs used to form credentials for connecting to the BWS. The URL format is https://<BES_URL>/enterprise/admin/util/ws.
BES Locale	Enter the country location of the BES. For example, en_US.
Authentication Method	Ensure that the Authentication Method field is set to Active Directory .
BES Username and Password	Enter the username and password needed to authenticate with the BES in the BES Username field and the BES Password field.
Domain	Enter a domain for the BES in the Domain field.

Setting	Description
Organization ID	Enter the applicable ID associated with the BES in the Organization ID field. This entry is typically 0 .
Sync Applications	Enable Sync Applications if you want to pull a list of applications from BlackBerry devices registered with the BES and Save the settings.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / QNX / Hub Settings

The QNX Hub settings page lets you configure options related to QNX devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

General

Setting	Description
Device ID Algorithm	Set the unique device identification algorithm used on the device.
Heartbeat Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits before checking-in with the Workspace ONE UEM console.
Data Sample Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to collect data from the device.
Data Transmit Time Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to send data to the UEM console.

Application List

Setting	Description
Applications Poll Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to check for new applications.

Certificate List

Setting	Description
Certificates Poll Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to check for new certificates.

Remote Management

Setting	Description
Mode	<p>Select the Mode to define how the remote management applet and the device communicate over the network.</p> <ul style="list-style-type: none"> ■ Off – Communication happens directly between the applet and the device. This mode is used when the computer that has the applet and the device you want to remotely manage are on the same network or virtual network. ■ Inbound – This is a legacy setting for the Remote Management Tunnel Server. ■ Outbound – This is a legacy setting for the Remote Management Tunnel Server. ■ WebSocket – Communication flows from the device to the applet. There is no direct connection available between the applet and the device. The applet and the device both proactively establish connections with the tunnel server. Use this when the device and the tunnel server are on different networks and the device can connect to the tunnel server on a public IP, for instance a device out in the field and the applet and tunnel located in a central location.
Enable Encryption	Enable to encrypt the data sent during remote management with AES 128 bit encryption.
Passphrase	Enter a passphrase used for authentication between the applet and the Workspace ONE Intelligent Hub.
Remote Management Port	<p>Enter the port used to communicate between the Remote Management Hub and the Tunnel Agent on the end user device.</p> <p>This port is responsible for catching the different frames on the device for use with screen sharing. The default port is 7775 and should not be changed unless port 7775 is in use for other uses in your organization.</p>
Device Log Level	Set the level of verbosity for the device logs when using the remote control application.
Log Folder Path	Enter the folder path for storing the device log.
Max Sessions	Enter the maximum number of sessions allowed through remote management.
Number of Retries	The number of retries allowed before communication attempts stop. This setting is available when WebSocket is selected as the Mode .
Retry Frequency (Seconds)	The amount of time between attempts to communicate. This setting is available when WebSocket is selected as the Mode .
Heart Beat Interval (Seconds)	The amount of time (in seconds) that passes between status updates are sent from the device. This setting is available when WebSocket is selected as the Mode .
Connection Loss Retry Frequency (Seconds)	The amount of time (in seconds) that passes between attempts to reestablish connection. This setting is available when WebSocket is selected as the Mode .

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Tizen / Hub Settings

The Tizen Hub Settings page lets you configure various options that affect the Tizen Hub mobile app. Adjusting these intervals can impact battery life, with smaller values equating to more frequent pings and greater power consumption.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Beacon Interval (min)	Enter the heartbeat time interval, which is how frequently the Workspace ONE Intelligent Hub checks in with the Workspace ONE UEM server. Reports beacon data to the Workspace ONE UEM console.
Data Sample Interval (min)	Enter the data sample time interval, which is how frequently the Workspace ONE Intelligent Hub collects data from the device.
Data Transmit Interval (min)	Enter the data transmit time interval, which is how frequently the Workspace ONE Intelligent Hub sends data to the AirWatch server.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Chrome OS / Hub Settings

The Chrome OS Hub Setting page lets you to configure the settings for the Workspace ONE Intelligent Hub for Chrome OS devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

To access the Workspace ONE Intelligent Hub settings page, navigate to **Groups & Settings > All Settings > Devices & Users > Chrome OS > Hub Settings**.

Setting	Description
Beacon Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will check in with the Workspace ONE UEM console.
Data Sample Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will collect a data sample from the device.
Data Transmit Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will transmit the collected data sample to the console.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Auto-Discovery

The Windows Auto-Discovery (WADS) settings page lets you set the type of WADS deployment you want to use and configure the related options. Windows Auto-Discovery is a service that allows users to enroll using only their email address and removes the need for end users to enter in a server address and a group identifier.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Auto-Discovery Mode – Select whether to use an on-premises WADS solution or to use Workspace ONE UEM Cloud-Hosted WADS.

- **On-Premises**
 - **Download Windows Auto-Discovery Installer** – Select to download the installer for creating an on-premises WADS solution.
- **Cloud-Hosted**
 - **Register Domain for Windows Auto-Discovery** – Select to launch the domain registry wizard for configuring a cloud-hosted WADS solution.

Devices & Users / Windows / Windows Rugged / Hub Application

The Windows Rugged Hub Application settings page lets you configure the options for downloading the specific Workspace ONE Intelligent Hub for Windows Rugged devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Use Default Cab	<p>Enable to use the default Workspace ONE Intelligent Hub for Windows Rugged cab file available from the Workspace ONE UEM console. Disable this option to use custom cabs you upload.</p> <ul style="list-style-type: none"> ■ Fully qualified path on local server to the Workspace ONE Intelligent Hub files for Windows Rugged devices – Enter the file path on the local server for the default cab if you enable the default cab.
Add Application	<p>Select to upload a custom cab file to push to Windows Rugged devices.</p> <ul style="list-style-type: none"> ■ Platform – Choose the cab file's specific OS. This option allows you to upload different cabs for different operating systems that your Windows Rugged devices use.
WM enrollment cab	Select the custom cab you want to push to devices running Windows Mobile.

Setting	Description
CE enrollment cab	Select the custom cab you want to push to ARM-based devices running Windows CE.
x86 CE enrollment cab	Select the custom cab you want to push to x86-based devices running Windows CE.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Rugged / Hub Settings

The Windows Rugged Hub Settings page lets you configure the options for the Workspace ONE Intelligent Hub for Windows Rugged devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

General

Setting	Description
Device ID Algorithm	Set the unique device identification algorithm used on the device. <ul style="list-style-type: none"> ■ Device ID Algorithm 3 – Hub uses the OS-provided API to generate the UDID. ■ Device ID Algorithm 5 – Along with the OS-provided API, the Workspace ONE Intelligent Hub uses the MAC ID of the device to generate the UDID. ■ Device ID Algorithm 6 – Together with the OS-provided API and the MAC ID of the device, the Workspace ONE Intelligent Hub also uses the serial number of the device to generate the UDID.
Heartbeat Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits before checking in with the Workspace ONE UEM console.
Data Sample Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to collect data from the device.
Data Transmit Time Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to send data collected from the device to the UEM console.
Check-In on Condition (Event)	Enable to limit the Workspace ONE Intelligent Hub to check-in or beacon to the UEM console only when certain conditions (Wi-Fi connection, AC Power, or NW Adapter) are met. This helps reduce bandwidth issues as devices typically meet the condition when they are stored for after hours.

Shared Devices (Check-in / Check-out)

Setting	Description
Enable Shared Device Mode	Select this check box to enable shared device functionality.

Notifications

Setting	Description
Enable Hub Installation Complete Notification	Select this check box to enable or disable notifications for Hub installation completion.
Enable Product Install Status Notification	Select this check box to enable or disable notifications through the Workspace ONE Intelligent Hub for product installation completion.

Location

Setting	Description
Collect Location Data	Enable to allow the to determine the device location based on a device's Wi-Fi network. When available, the Workspace ONE Intelligent Hub will report the location to the Workspace ONE UEM console using the Data Transmit Interval.

Application List

Setting	Description
Applications Poll Interval (min)	Set the time interval (in minutes) at which the applications list for each device will refresh on the Workspace ONE UEM console.

Certificate List

Setting	Description
Certificate Poll Interval (min)	Set the time interval at which the certificate list for each device will refresh on the Workspace ONE UEM console.

Proxy

Setting	Description
Proxy Configuration	Enable to allow the configuration of a proxy settings.

Application Manager Package Scheduler (Only for AirWatch 3.3 Hub)

These settings are for the legacy Workspace ONE Intelligent Hub v3.3.

Use the **APPLICATION MANAGER SCHEDULER** to define a schedule for devices with the Workspace ONE Intelligent Hub v3.3+ to retrieve products provisioned on schedule.

Setting	Description
Add	Select to create schedules for provisioning products using Products (Legacy).
Application Manager Scheduler	Select the hour the product begins to push to devices.
Randomization Window (min)	Select the amount of time the product is pushed. The order of devices is randomized.

Remote Management

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	<p>Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin.</p> <ul style="list-style-type: none"> ■ Enter a Seek Permission Message that the end user sees when a remote request is sent. ■ Enter the Yes Caption message for the accept button the end user sees on the Seek Permission request. ■ Enter the No Caption message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	<p>Enter the port used to communicate between the Remote Management Hub and the Tunnel Agent on the end-user device.</p> <p>This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.</p>
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

Product Provisioning

Settings	Descriptions
Job Log Level	<p>Select the level of detail your job logs contain. You can choose between the following options.</p> <p>Error – The log contains errors only. This setting produces the smallest amount of detail.</p> <p>Warning – The log contains errors and all warnings.</p> <p>Information – The log contains all errors, all warnings, and all supplemental information.</p> <p>Verbose – The log contains all of the above plus the entire ledger of exchanges between the device and the server, no matter how trivial. Select this option for troubleshooting purposes. This option produces the largest log.</p>

Wipe

Settings	Descriptions
Retain Hub Executables After Enterprise Wipe	Enable to keep the Workspace ONE Intelligent Hub executable files after an enterprise wipe command is issued to the device.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Rugged / Power on Password

With the Windows Rugged Power On Password settings, you can configure the options for requiring a password on a device startup.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Force Password Expiration	Enable this setting to force the password to expire so that the user must change the password.
View Power On Password	Enable this setting to allow the user to see the password that they enter.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Rugged / Metrics

The Windows Rugged Metrics settings page lets you configure the options for downloading the MotoDC metrics application as well as configure the metrics collected.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Download MotoDC	Select to download the MotoDC cab to collect device metrics. You can set which metrics to collect below the download link.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Rugged / Advanced

The Windows Desktop Advanced settings page lets you configure the various advanced options for the Workspace ONE Intelligent Hub for Windows Rugged.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Path to App Update	Enter the default directory for app updates on devices.
Intermec Reboot Exe	Enter the default path to the reboot executable (Intermec Devices).

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Phone / Intelligent Hub Application

The Windows Phone Intelligent Hub Application settings page lets you configure the options for hosting the Workspace ONE Intelligent Hub for Windows Phone devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Hub Download URL	Enter the Workspace ONE Intelligent Hub for Windows Phone download URL.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Phone / Hub Settings

The Windows Phone Hub Settings page lets you configure the options for the Workspace ONE Intelligent Hub for Windows Phone devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

DM Sessions Settings

Setting	Description
Enterprise Name	Set the Enterprise Name that the Workplace feature of the Windows Phone device shows when a device is enrolled in Workspace ONE UEM.
Device Sync Interval (min)	Set the time (in minutes or hours) the native DM client waits before checking in with the Workspace ONE UEM console.

Workspace ONE Intelligent Hub Settings

Setting	Description
Heartbeat Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits before checking in with the UEM console.
Data Sample Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits to collect data from the device.
Profile Refresh Interval (min)	Set the frequency (in minutes) the profile list of each device refreshes on the server.
Enable Passcode	Enable the use of a passcode to access the Workspace ONE Intelligent Hub settings on the device.
Administrative Passcode	Enter the administrative passcode to enter for access to Hub settings on the device.
Collect Location Data	Enable to collect the location data from the device. The location is determined based on the Wi-Fi network of the device. When located data is available, the Workspace ONE Intelligent Hub sends the location data to the console at the Transmit Interval.
GPS Sample Interval (min)	Set the time (in minutes) the Workspace ONE Intelligent Hub waits before collecting GPS data from the device.
Enable Push Notification Services	Enable to allow the console to send Push Notifications to devices.

Enterprise App Management

Setting	Description
Enable Enterprise App Management	Enable to use the Enterprise Application Management feature for pushing internal applications to Windows Phone devices.
Upload Enterprise Token	Select Change to upload an Enterprise Token for use with Enterprise Application Management.

Important This token expires annually. If the token is expired and still enabled, you cannot enroll into this organization group.

About Page Configuration

Setting	Description
Customize About Page Content	Enable to display a text field for customizing the Workspace ONE Intelligent Hub about page.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Phone / Company Hub Settings

The Windows Phone Company Hub settings page lets you configure the options for using the company hub applications with Windows Phone.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Enable Company Hub	Enable to use the Company Hub functionality to silently push an enhanced Workspace ONE Intelligent Hub to devices after enrollment. Company Hub requires the use of Enterprise Application Tokens.
Company Hub Name	Enter the display name of the Company Hub application.
Company Hub Application	Select the Company Hub application from the drop-down list of all Windows Phone internal application.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Phone / MDM Sample Schedule

The Windows Phone MDM Sample Schedule settings page lets you configure the time intervals at which certain data samples are sent to the Workspace ONE UEM console server.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Application List Sample	Enter the frequency by which application list information is refreshed on the Workspace ONE UEM server.
Certificate List Sample	Enter the frequency by which certificate list information is refreshed on the Workspace ONE UEM server.
Device Details Sample	Enter the frequency by which device information is refreshed on the Workspace ONE UEM server.
Email EAS Active Sync Sample	Enter the frequency by which EAS information is refreshed on the Workspace ONE UEM server.
Enterprise Application Token	Enter the frequency by which enterprise application token information is refreshed on the Workspace ONE UEM server.
Internet Email Accounts Sample	Enter the frequency by which internet email account information is refreshed on the Workspace ONE UEM server.
Security Information Sample	Enter the frequency by which security information is refreshed on the Workspace ONE UEM server.
Health Attestation Sample	Enter the frequency by which health attestation information is refreshed on the Workspace ONE UEM server.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Phone / Windows Health Attestation

The Health Attestation settings page allows you to configure the compromised status definitions for Windows Phone devices.

Settings	Descriptions
Compromised Status Definition	
Use Custom Server	Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the Server URL field.
Server URL	Enter the URL for your custom Health Attestation server.

Settings	Descriptions
Secure Boot Disabled	<p>Enable to flag compromised device status when Secure Boot is disabled on the device.</p> <p>Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files.</p>
Attestation Identity Key (AIK) Not Present	<p>Enable to flag compromised device status when the AIK is not present on the device.</p> <p>Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.</p>
Data Execution Prevention (DEP) Policy Disabled	<p>Enable to flag compromised device status when the DEP is disabled on the device.</p> <p>The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. DEP is enforced by both hardware and software.</p>
BitLocker Disabled	<p>Enable to flag compromised device status when BitLocker encryption is disabled on the device.</p>
Code Integrity Check Disabled	<p>Enable to flag compromised device status when the code integrity check is disabled on the device.</p> <p>Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software.</p>
Early Launch Anti-Malware Disabled	<p>Enable to flag compromised device status when the early launch anti-malware is disabled on the device.</p> <p>Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.</p>
Code Integrity Version Check	<p>Enable to flag compromised device status when the code integrity version check fails.</p>
Boot Manager Version Check	<p>Enable to flag compromised device status when the boot manager version check fails.</p>
Boot App Security Version Number Check	<p>Enable to flag compromised device status when the boot app security version number does not meet the entered number.</p>
Boot Manager Security Version Number Check	<p>Enable to flag compromised device status when the boot manager security version number does not meet the entered number.</p>
Advanced Settings	<p>Enable to configure advance settings in the Software Version Identifiers section.</p>
Software Version Identifiers	
Code Integrity Policy Hash Check	<p>Enable to define a whitelist of known, valid hash values for the Code Integrity software. If the hash is not a whitelisted value, health attestation compliance fails.</p>
Secure Boot Config Policy Hash Check	<p>Enable to define a whitelist of known, valid hash values for the Secure Boot Config software. If the hash is not a whitelisted value, health attestation compliance fails.</p>
PCR0 Check	<p>Enable to define a whitelist of known, valid measurements for the PCR0 Check software. This measurement checks the BIOS trusted code to ensure that it has not been compromised. If the measurement is not a whitelisted value, health attestation compliance fails.</p>

Devices & Users / Windows / Windows 7 / Hub Application

The Windows 7 Hub Application settings page lets you configure the options for hosting the Workspace ONE Intelligent Hub for Windows 7 devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Fully qualified path on local server to the Workspace ONE Intelligent Hub files for Windows PC	Enter the file path on the local server to the Workspace ONE Intelligent Hub files for the Workspace ONE Intelligent Hub for Windows 7 devices.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows 7 / Hub Settings

The Windows 7 Hub Settings page lets you configure the options for the Workspace ONE Intelligent Hub for Windows 7 devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Beacon Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will check in with the Workspace ONE UEM console.
Data Sample Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will collect a data sample from the device.
Data Transmit Interval (min)	Enter the time interval (in minutes) at which the Workspace ONE Intelligent Hub will transmit the collected data sample to the console. This settings also controls how often the Workspace ONE Intelligent Hub checks for a new automatic upgrade if enabled.
Block Enrollment if Windows Genuine validation fails	Enable to block devices with non-genuine copies of Windows Operating Systems from enrolling into Workspace ONE UEM. <ul style="list-style-type: none"> ■ If a device is enrolled and the Workspace ONE Intelligent Hub detects the Windows copy is not genuine, the Workspace ONE Intelligent Hub will send an Enterprise Wipe command to the device. ■ If a device attempts to enroll and the copy of Windows is not genuine, a Non-Compliance message will display and immediately unenroll a device.

Setting	Description
Enforce Passcode Profile	Enable to force the Workspace ONE Intelligent Hub to prompt end users for password changes when a passcode profile is installed or updated. This option does not apply to domain-joined devices.
Windows Agent Automatic Updates	Enable to automatically update the Workspace ONE Intelligent Hub when an update becomes available.

Remote Management

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	<p>Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin.</p> <ul style="list-style-type: none"> ■ Enter a Seek Permission Message that the end user sees when a remote request is sent. ■ Enter the Yes Caption message for the accept button the end user sees on the Seek Permission request. ■ Enter the No Caption message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	<p>Enter the port used to communicate between the Remote Management Hub and the Tunnel Agent on the end-user device.</p> <p>This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.</p>
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / General

The Windows Desktop General settings page lets you configure the options for using Powershell with Windows 8.0/RT devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Settings	Descriptions
PowerShell URL	Enter the URL where the Workspace ONE UEM console can access your PowerShell service.
Username	Enter the username the UEM console needs to communicate with the PowerShell service.
Password	Enter the password the UEM console needs to communicate with the PowerShell service.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / Hub Application

The Windows Desktop Hub Application page lets you configure the various options for the Unified Agent.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Publish Workspace ONE Intelligent Hub	Enable to use the Workspace ONE Intelligent Hub for Windows 8.1 devices to configure device security and protection settings.
Device Ownership Type	Select the ownership types you want to require enrolling with the Workspace ONE Intelligent Hub enrollment method.
Unified Agent Automatic Updates	Enable to automatically update the Workspace ONE Intelligent Hub when a new version is available.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / Hub Settings

The Windows Desktop Hub Settings page lets you configure the various options for the Workspace ONE Intelligent Hub for Windows Desktop devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Modern Hub

Settings	Descriptions
Heartbeat Interval (min)	Defines the intervals at which the Workspace ONE Intelligent Hub and the Workspace ONE UEM console confirm a continued connection and synchronize.
Data Sample Interval (min)	Defines the intervals at which the Workspace ONE Intelligent Hub takes samples of data.
Administrative Passcode	Sets the passcode to access administrative settings on the device.
MDM Channel Security	Defines the app layer security between Workspace ONE UEM and the Workspace ONE Intelligent Hub. This secure channel uses the enrollment certificate to sign, encrypt, or sign and encrypt communications between the UEM console and the Workspace ONE Intelligent Hub.

Workspace ONE Intelligent Hub

Setting	Description
Data Sample Interval (min)	Defines the intervals at which the Workspace ONE Intelligent Hub takes a sample of data from the device.

Remote Management

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	<p>Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin.</p> <ul style="list-style-type: none"> ■ Enter a Seek Permission Message that the end user sees when a remote request is sent. ■ Enter the Yes Caption message for the accept button the end user sees on the Seek Permission request. ■ Enter the No Caption message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	<p>Enter the port used to communicate between the Remote Management Hub and the Tunnel Agent on the end-user device.</p> <p>This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.</p>

Setting	Description
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / App Deployments

The Windows Desktop App Deployments page lets you configure software package deployment for Win32 applications.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Software Package Deployment	Select Enabled to enable the ability to deploy Win32 applications from the Apps & Books section so that you can use the application life cycle flow that exists for all internal applications.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / Enterprise Apps

The Windows Desktop Enterprise Apps settings page lets you configure the various options for Enterprise Application Management.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Enable Enterprise Application Management	Enable to use the Enterprise Application Management feature for pushing internal applications to Windows Desktop devices.
Side Loading Key	Enter the Side Loading Key required for pushing internal applications to Windows Desktop devices.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / Windows Sample Schedule

The Windows Desktop Sample Schedule settings page lets you configure the time intervals at which certain data samples are sent to the Workspace ONE UEM console server.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Device Details Sample	Enter the frequency by which device information is refreshed on the Workspace ONE UEM server.
Security Information Sample	Enter the frequency by which security information is refreshed on the Workspace ONE UEM server.
Browser Information Sample	Enter the frequency by which browser information is refreshed on the Workspace ONE UEM server.
Application List Sample	Enter the frequency by which application information is refreshed on the Workspace ONE UEM server.
Certificate List Sample	Enter the frequency by which certificate information is refreshed on the Workspace ONE UEM server.
Restriction Information Sample	Enter the frequency by which restriction information is refreshed on the Workspace ONE UEM server.

Setting	Description
Health Attestation Sample	Enter the frequency by which health attestation information is refreshed on the Workspace ONE UEM sever.
Update Sample	Enter the frequency by which Windows update information is refreshed on the Workspace ONE UEM server.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Windows / Windows Desktop / Windows Health Attestation

The Health Attestation settings page allows you to configure the compromised status definitions for Windows Desktop devices.

Settings	Descriptions
Compromised Status Definition	
Use Custom Server	Select to configure a custom server for Health Attestation. This option requires a server running Windows Server 2016 or newer. Enabling this option displays the Server URL field.
Server URL	Enter the URL for your custom Health Attestation server.
Secure Boot Disabled	Enable to flag compromised device status when Secure Boot is disabled on the device. Secure Boot forces the system to boot to a factory trusted state. When Secure Boot is enabled, the core components used to boot the machine must have the correct cryptographic signatures that the OEM trusts. The UEFI firmware verifies the trust before it allows the machine to start. Secure boot prevents the startup if any it detects any tampered files.
Attestation Identity Key (AIK) Not Present	Enable to flag compromised device status when the AIK is not present on the device. Attestation Identity Key (AIK) is present on a device, it indicates that the device has an endorsement key (EK) certificate. It can be trusted more than a device that does not have an EK certificate.
Data Execution Prevention (DEP) Policy Disabled	Enable to flag compromised device status when the DEP is disabled on the device. The Data Execution Prevention (DEP) Policy is a memory protection feature built into the system level of the OS. The policy prevents running code from data pages such as the default heap, stacks, and memory pools. DEP is enforced by both hardware and software.
BitLocker Disabled	Enable to flag compromised device status when BitLocker encryption is disabled on the device.
Code Integrity Check Disabled	Enable to flag compromised device status when the code integrity check is disabled on the device. Code integrity is a feature that validates the integrity of a driver or system file each time it is loaded into memory. Code integrity checks for unsigned drivers or system files before they load into the kernel. The check also scans for users with administrative privileges running system files modified by malicious software.
Early Launch Anti-Malware Disabled	Enable to flag compromised device status when the early launch anti-malware is disabled on the device. Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize.

Settings	Descriptions
Code Integrity Version Check	Enable to flag compromised device status when the code integrity version check fails.
Boot Manager Version Check	Enable to flag compromised device status when the boot manager version check fails.
Boot App Security Version Number Check	Enable to flag compromised device status when the boot app security version number does not meet the entered number.
Boot Manager Security Version Number Check	Enable to flag compromised device status when the boot manager security version number does not meet the entered number.
Advanced Settings	Enable to configure advance settings in the Software Version Identifiers section.
Software Version Identifiers	
Code Integrity Policy Hash Check	Enable to define a whitelist of known, valid hash values for the Code Integrity software. If the hash is not a whitelisted value, health attestation compliance fails.
Secure Boot Config Policy Hash Check	Enable to define a whitelist of known, valid hash values for the Secure Boot Config software. If the hash is not a whitelisted value, health attestation compliance fails.
PCR0 Check	Enable to define a whitelist of known, valid measurements for the PCR0 Check software. This measurement checks the BIOS trusted code to ensure that it has not been compromised. If the measurement is not a whitelisted value, health attestation compliance fails.

Devices & Users / Peripherals / Server

The Peripherals Server settings page lets you configure several options related to the management of printers connected to your Workspace ONE UEM environment.

The following settings display after you select **Add Printer Server**.

Setting	Description
HMAC Token	The HMAC key is auto-generated and will be used to associate the print server to the appropriate organization group in Workspace ONE UEM. This key will need to be entered into the relevant Print Server configuration file.
User Id	Select the appropriate enrollment user that will be associated to the Print Server. This user is typically an AirWatch Administrator and may be associated to multiple Print Servers.
Service Uid	Enter the ID of the print server which identifies it uniquely.

Devices & Users / Peripherals / Sample Schedule

The Peripherals Sample Schedule settings page lets you configure the time intervals at which device details samples from peripheral devices are sent to the Workspace ONE UEM server.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Device Details Sample	Enter the time range (days or hours) to collect peripheral device detail samples. Days range from 1 to 48 and hours range from 1 to 30.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Advanced / Bulk Management

The Bulk Management settings page lets you determine the maximum number of devices that can be affected by a bulk management action performed by an administrator in the Workspace ONE UEM console. Next to each action, enter the maximum number of allowable device changes that you want to occur at once using bulk management.

Keep in mind that not all devices are capable of executing all available remote actions. The bulk action option will not be available if your selected devices include a device that cannot execute the action in question.

For example, if your Warm Boot maximum is set to 1000 and you select 500 devices to warm boot, if even one device out of the 500 selected can't handle a warm boot, the bulk action option will not be displayed. For more information, see **Device Actions by Platform** in the **VMware Workspace ONE UEM Mobile Device Management Documentation**.

Setting	Description
Query	Enter the maximum number of device queries you can run in a bulk command.
Send Message	Enter the maximum number of devices that can receive a bulk message.
Enterprise Wipe	Enter the maximum number of devices you may wipe in a bulk command.
Delete Device	Enter the maximum number of devices you may remove from Workspace ONE UEM as part of a bulk command.
Enterprise Reset	Enter the maximum number of devices you may invoke an enterprise reset in a bulk command.
Device Wipe	Enter the maximum number of devices you may wipe in a bulk command.
Lock Device	Enter the maximum number of devices you may lock in a bulk command.
GPS	Enter the maximum number of devices from which you may request GPS data in a bulk command.
Change Organization Group	Enter the maximum number of devices for which you may change the organization group in a bulk command.
Change Ownership	Enter the maximum number of ownership changes you may invoke upon devices as part of a bulk command.
Warm Boot	Enter the maximum number of devices you may invoke a warm boot operation in a bulk command.
Provision Now	Enter the maximum number of devices you may concurrently provision as part of a bulk command.
Shutdown and Reboot	Enter the maximum number of devices upon which you may invoke a shutdown and reboot bulk command.

Setting	Description
Do Not Disturb	Enter the maximum number of devices you may set to Do Not Disturb as part of a bulk command.
Assign/Unassign Tag	Enter the maximum number of devices to which you are able to add a bulk tag.
Enable Lost Mode	Enter the maximum number of devices for which you may enable lost mode in a bulk command.
Disable Lost Mode	Enter the maximum number of devices for which you may disable lost mode in a bulk command.
Custom Command	Enter the maximum number of devices upon which you may invoke a custom bulk command.
iOS Update	Enter the maximum number of iOS devices whose operating systems can be updated concurrently as part of a bulk command.

Devices & Users / Advanced / Custom Fields

The Custom Field Definitions settings page correlates with a legacy Workspace ONE Intelligent Hub for Windows Rugged devices. If you are using up-to-date versions of the Workspace ONE Intelligent Hub this setting page does not apply to you. You should not modify the settings on this page unless you know what they do and have talked to Workspace ONE UEM about modifying them.

Devices & Users / Advanced / Device Groups

Device Groups is a legacy setting that defines a group of devices without reference to their location. In the current version of Workspace ONE UEM, this functionality is much better served by making use of device tags or smart groups.

Setting	Description
Add New Device Group	<p>Select this button to display the Add New Device Group screen and complete the following options.</p> <ul style="list-style-type: none"> ■ Device Group – Required field used to label the device group. ■ Organization Group – Required field used to identify the OG in which this device group resides. ■ Location – This optional field allows you to define a single location for the device group, independent from the organization group. ■ Description – Enter a description of the device group's purpose.

Devices & Users / Advanced / Area

The Area settings page lets you add geofences or iBeacons for use in the Workspace ONE UEM console.

Workspace ONE UEM enables you to define your profile with a Geofencing Area. A geofence area limits the use of the device to specific areas including corporate offices, school buildings, and retail department stores. You can think of a geofence area as a virtual perimeter for a real-world geographic area.

For example, a geofence area with a 1-kilometer radius can apply to your office, while a much larger geofence area can apply approximately to an entire state. Once you have defined a geofence area you can apply it to profiles, SDK applications, and Workspace ONE UEM apps such as the VMware Content Locker, and more.

Table 3-1. Geofencing Area

Setting	Description
Area Name	Enter a name that represents your defined geofence in the listing.
Address	Enter a street address that serves as the epicenter of the geofence. Select the Click to Search button to send the entered address as a search parameter to Bing maps. If the search is successful, the correct address appears in the map displayed under the button.
Radius	Enter how large you want the geofence to be. You can select kilometers or miles. The default radius is 1 kilometer.
Map (dynamic image)	<p>You can select between three different views: Road (standard road map), Ariel (photorealistic view), and Bird's Eye (a three-dimensional modelled view).</p> <p>Select the Locate Me button to send your current location to the Bing map. You might be asked by your browser to approve/confirm sending the location.</p> <p>You can zoom the map's view in and out using the Plus and Minus icons.</p>

Devices & Users / Advanced / Tags

The tags settings page lets you add tags for use in the Workspace ONE UEM console. Tags allow you to easily identify a specific device without requiring a device profile, smart group or compliance policy and without requiring the creation of a note.

Devices & Users / Advanced / User Categories

User Categories is a legacy setting that defines a user or a group of users without reference to their location or role. In the current version of Workspace ONE UEM, this functionality is much better served by making use of child organization groups and user groups.

For Windows Rugged devices only, User Categories are the way to establish multi-user device staging. In such a case, you would create a User Category for each user that needs to share a single Windows Rugged device. You would then associate the Windows Rugged Launcher with the established User Categories, thereby effectively implementing multi-user device staging.

Select the **Add** button to create a user category and complete the following options.

Setting	Description
Name	Required field used to label the user category.
Description	Enter a description of the user category's purpose.

Devices & Users / Advanced / User Migration

The User Migration settings page lets customers with Basic Users intending to switch over to LDAP users employ the User Migration feature.

The User Migration tool provides an easy way to check existing Basic Users against current directory users and consolidate information throughout. Additionally, customers using Auth Proxy or legacy SAML who want to start utilizing user groups may employ the User Migration feature to update their users.

Devices & Users / Advanced / Unmanaged Device Wipe Protection

The Unmanaged Wipe Protection settings page lets you configure options that let you exert more control over how and when **unmanaged devices** can be wiped to avoid mass wiping devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Unmanaged Device Wipe Protection

Setting	Description
Wiped Devices	Enter the number of Wiped Devices that acts as your threshold for triggering wipe protection.
Within (minutes)	Enter the value for Within (minutes) which is the amount of time the wipes must occur to trigger wipe protection.
Email	<p>Select a message template to email to administrators.</p> <p>Create a message template for wipe protection by navigating to Groups & Settings > All Settings > Devices & Users > General > Message Templates and select Add. Next, select Device Lifecycle as the Category and Wipe Protection Notification as the Type. You can use the following lookup values as part of your message template.</p> <ul style="list-style-type: none"> ■ {EnterpriseWipeInterval} – The value of Within (minutes) on the settings page. ■ {WipeLogConsolePage} – A link to the Wipe Log page.
To	Enter the email addresses of administrators who must be notified. These administrators must have access to the Wipe Log page.
Allow Enterprise Wipes	Enable the enterprise wiping of unmanaged devices. The default setting is enabled.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Advanced / Managed Device Wipe Protection

The Wipe Protection settings page lets you configure options that let you exert more control over how and when **managed devices** can be wiped to avoid mass wiping devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Managed Device Wipe Protection

Setting	Description
Wiped Devices	Enter the number of Wiped Devices that acts as your threshold for triggering wipe protection.
Within (minutes)	Enter the value for Within (minutes) which is the amount of time the wipes must occur to trigger wipe protection.
Email	<p>Select a message template to email to administrators.</p> <p>Create a message template for wipe protection by navigating to Groups & Settings > All Settings > Devices & Users > General > Message Templates and select Add. Next, select Device Lifecycle as the Category and Wipe Protection Notification as the Type. You can use the following lookup values as part of your message template.</p> <ul style="list-style-type: none"> ■ {EnterpriseWipeInterval} – The value of Within (minutes) on the settings page. ■ {WipeLogConsolePage} – A link to the Wipe Log page.
To	Enter the email addresses of administrators who must be notified. These administrators must have access to the Wipe Log page.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Devices & Users / Advanced / Profile Options

The Profile Options settings page lets you enable a setting that lets administrators select the **Interactive Assignment Type** for device profiles. The Interactive settings means the only way a profile can be installed on a device is if the user logs in to the Self-Service Portal and initiates the installation.

Apps

4

This section provides information about Workspace ONE UEM Apps settings.

The Workspace ONE UEM Apps settings are categorized into the following:

- App Scan
- Application Integration
- Browser
- Workspace ONE
- Container
- Inbox
- Video
- Settings and Policies

This chapter includes the following topics:

- [Apps / App Scan / Third-Party Integration](#)
- [Apps / Application Integration / TouchDown](#)
- [Apps / Browser](#)
- [Apps / Workspace ONE / Catalog / General](#)
- [Apps / Workspace ONE / Catalog / Standalone Catalog](#)
- [Apps / Workspace ONE / App Restrictions](#)
- [Apps / Workspace ONE / Application Categories](#)
- [Apps / Workspace ONE / External App Repository](#)
- [Apps / Workspace ONE / Application Removal Protection](#)
- [Apps / Workspace ONE / Catalog / Featured Applications](#)
- [Devices & Users / Apple / VPP Managed Distribution](#)
- [Apps / Workspace ONE / Paid Public Applications](#)
- [Apps / Container](#)

- [Apps / Inbox](#)
- [Apps / Video](#)
- [Apps / Settings and Policies / Security Policies](#)
- [Apps / Settings and Policies / Settings](#)
- [Apps / Settings and Policies / Profiles](#)
- [Apps / Microsoft Intune® App Protection Policies](#)

Apps / App Scan / Third-Party Integration

The Third-Party Integration setting allows you to add your App Scan service information to the UEM console so that the systems can share applications and scan results.

Note Ensure that you are in the desired organization group that is a **Customer** type.

Common Settings

Setting	Description
Enable Third Party App Scan Analysis	Select to enable communication between Workspace ONE UEM and the App Scan Vendor and to display available options on the page.
Choose App Scan Vendor	Select the applicable third-party vendor.

Setting	Description
Save	Saves configurations and syncs with the App Scan Vendor when the Workspace ONE UEM scheduler task runs.
Sync Now	Saves configurations and begins a manual sync with the App Scan Vendor without waiting for the scheduler task to run.

Veracode Mobile Application Reputation Service (MARS) Settings

Setting	Description
Veracode Username	Enter the username for your Veracode MARS.
Veracode Password	Enter the password for the username to authenticate to your Veracode MARS.
Veracode REST API URL	Enter the URL for your Veracode MARS to direct Workspace ONE UEM to the service.

Setting	Description
Enable Email Notification	Displays the Application Group Creation area to configure the system to send notifications to admins when analysis creates new app groups in Workspace ONE UEM.
Send Email To	Enter email addresses to receive notifications about new app groups created by analysis. Use a comma to separate addresses.
Message Template	Use Message Preview to see the email that the system sends upon the creation of new app groups using the Vendor Application Group Creation Notification template.

Palo Alto Networks WildFire Settings

Setting	Description
WildFire API Key	Enter the key for your WildFire system so Workspace ONE UEM can send application hashes directly to WildFire.

Pradeo Security System

Setting	Description
Pradeo Username	Enter the username for your Pradeo.
Pradeo Password	Enter the password for the username to authenticate to your Pradeo.
Pradeo REST API URL	Enter the URL for your Pradeo to direct Workspace ONE UEM to the service.

Setting	Description
Enable Email Notification	Displays the Application Group Creation area to configure the system to send notifications to admins when analysis creates new app groups in Workspace ONE UEM.
Send Email To	Enter email addresses to receive notifications about new app groups created by analysis. Use a comma to separate addresses.
Message Template	Use Message Preview to see the email that the system sends upon the creation of new app groups using the Vendor Application Group Creation Notification template.

Appthority

Setting	Description
Appthority Username	Enter the username for your Appthority.
Appthority Password	Enter the password for the username to authenticate to your Appthority.
Appthority REST API URL	Enter the URL for your Appthority to direct Workspace ONE UEM to the service.

Setting	Description
Enable Email Notification	Displays the Application Group Creation area to configure the system to send notifications to admins when analysis creates new app groups in Workspace ONE UEM.
Send Email To	Enter email addresses to receive notifications about new app groups created by analysis. Use a comma to separate addresses.
Message Template	Use Message Preview to see the email that the system sends upon the creation of new app groups using the Vendor Application Group Creation Notification template.

Apps / Application Integration / TouchDown

The NitroDesk TouchDown settings page lets you configure some options related to the NitroDesk TouchDown email client.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
TouchDown for iOS Type	Select the type of iOS Touchdown app. Options are Standard, Government, and Custom.
	The ID used by iOS to uniquely identify an application. It follows the reverse DNS format.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Browser

The Browser settings page lets you configure settings related to the VMware Browser app.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Browser Settings

Setting	Description
Settings and Policies	
Application Profile	<p>Select an application profile to apply SDK functionality to your app.</p> <ul style="list-style-type: none"> ■ Default – Allow applications to use the default security policies and settings defined under Apps and Books > Settings > Settings and Policies. ■ Custom – Override default settings and apply custom profiles. Custom profiles use the security policies and settings defined under Apps and Books > Settings > Settings and Policies > Profiles.
iOS SDK Profile	Select the appropriate profile from the drop-down menu that appears when you enable a Custom Application Profile to override default SDK settings.
Android SDK Profile	Select the appropriate profile from the drop-down menu that appears when you enable a Custom Application Profile to override default SDK settings.
Use Legacy Settings and Policies	Enable to configure settings and policies for legacy web only.
Disable Copy	(Legacy web only) Enable this option to prevent copying from device. Configure this option under Data Loss Prevention in Settings > Apps > Settings and Policies .

Setting	Description
Disable Printing	(Legacy web only) Enable this option to prevent printing from device. Configure this option under Data Loss Prevention in Settings > Apps > Settings and Policies .
Force Downloads To Open in Content Locker	(Legacy web only) Enable this option to open the force downloaded documents in Content Locker. Configure this option under Data Loss Prevention in Settings > Apps > Settings and Policies .
Enable AW Tunnel Proxy	(Legacy web only) Enable AW App Tunnel Proxy to access internal network. Configure this option under Data Loss Prevention in Settings > Apps > Settings and Policies .
iOS SDK Profile (Legacy)	Select the appropriate iOS SDK profile from the drop-down menu for the legacy web.
General	
Accept Cookies	Enable to accept cookies from websites viewed in the Workspace ONE Web.
Clear Cookies Upon Exit	Enable to clear cookies when the app fully closes.
Clear Cookies and History if Idle	Enable to clear cookies and history if the web is idle for x minutes.
Clear Cookies and History if Idle for (mins)	Set the idle time in minutes to a value between 0.5 and 60 to ensure cookies and history are clear.
Remember History	Enable to keep track of the sites visited by the user.
Remember History From	Select the length of time you want the app to remember history to from the drop-down menu.
Caching	Enable to enhance web performance and reduce perceived lag time. Disable to protect browsing data on compromised devices.
Allow Connection to Untrusted Sites	Disable if navigating to untrusted sites is a security concern for your organization. Enable to give end users maximum navigation flexibility and ease of use.
Sync User Bookmarks	Enable this to sync bookmarks across various devices of the same user.
Default View Mode	Set the default view mode for Workspace ONE Web. Select Desktop to set desktop as the default view mode. When selected, the Workspace ONE Web renders the web pages in desktop mode if the websites supports the mode.
Mode	
Kiosk Mode	Enable for Workspace ONE Web to function in Kiosk Mode . Kiosk Mode removes the navigation bar and limits browsing to the homepage and its available links.
Return Home After Inactivity	Direct the Workspace ONE Web back to the home page after a period of Inactivity (min) . The values can be greater than or equal to 0.5 minutes.
Clear Cookies and History with Home	Prevent users from accessing the previous user's secure information after they finish using the Workspace ONE Web.
Enable Multiple Tabs Support	You can have multiple tabs opened within kiosk mode. This feature is supported only on iOS and Android devices.
Home Page URL	Define the URL displayed when the web starts. Leave this field blank to display a 'Recently Visited' page by default.
Selection Mode	Allow to limit browsing to domains white listed in the Allowed Site URLs field. Deny to allow browsing to all sites except those blacklisted in the Denied Site URLs field.

Setting	Description
Allowed/Denied Site URLs	<p>Utilize the following recommendations to whitelist allowed domains and blacklist denied domains.</p> <ul style="list-style-type: none"> ■ Define domain names without including full URLs. The Workspace ONE Web filters by domain only, not by folder or page level. ■ Separate domains with a space, comma, or a new line. ■ Define wildcards as part of the domains; listing items from most general to specific. Example: *google.com is more general than http://yahoo.com. <p>Entering *.google.com whitelists <text>.google.com, but it does not allow access to http://google.com.</p> <ul style="list-style-type: none"> ■ Leave out the scheme (http:// or https://) to test the domain for both schemes. Include the scheme to limit testing to the specified scheme. ■ You can enter Port value separately. Restricted URL can contain the complete path, for example, http:// google.com:9191.
Allow IP Browsing	<p>Select to whitelist IP addresses for browsing.</p> <p>A user can navigate to a whitelisted IP address even if the actual domain for the IP address was included in the Denied Site URL listing.</p>
Allowed IP Addresses	<p>Whitelist IP addresses using the following recommendations:</p> <ul style="list-style-type: none"> ■ Enter values in IPv4 formatting with four octets each separated by a period. ■ Enter wildcards to whitelist octets. Adding an entry that includes a * in each octet allows browsing to any IP address.
Terms of Use	
Required Terms of Use	<p>Select the appropriate agreement from the drop-down menu. For all internal Workspace ONE UEM apps, including the Workspace ONE Web, you can implement a single Terms of Use Agreement for end users to accept. This agreement applies to all Workspace ONE UEM internal applications, and eliminates the need for end users to accept the same agreement multiple times, across apps.</p> <p>You can configure and manage your Terms of Use Agreements by navigating to Groups and Settings > All Settings > System > Terms of Use. For more information, please see the VMware AirWatch Mobile Device Management Guide on docs.vmware.com.</p>

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Bookmarks

Setting	Description
for Predefined Bookmarks in Browser	Configure bookmarks to display as a URL address or with a friendly name.
Name	Provide text in this field to display as the friendly name. Leave this field blank to display the URL as the bookmark name.
URL	Provide the bookmark URL.
	Select to add additional bookmarks.

Notification

Do not configure any settings on this tab unless you have been provided with specific instructions on how to complete the fields from Workspace ONE UEM.

Apps / Workspace ONE / Catalog / General

The Catalog / General settings page lets you configure several options related to the AirWatch App Catalog.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Authentication

Setting	Description
Require Authentication	Require users to log in with their username and password before they can access the app catalog. This option is disabled by default which sets Workspace ONE UEM to require no authentication to access the app catalog.
Reauthenticate	<p>Select a reauthentication option.</p> <ul style="list-style-type: none"> ■ Never - Keep User Signed In – Keeps users signed in and does not require them to log in each time. ■ After XX day(s) – Require users to authenticate (log in) after a set number of days. <p>Users still have to reauthenticate if they clear cookies on their devices, even with this option enabled.</p>

Publishing

Setting	Description
Catalog Title	Enter a name for your app catalog. This title appears on the home screen of the device.
Platforms	Select the supported platforms for your app catalog. If this is enabled for the platform, the profile gets pushed to the device.
Icon	<p>Upload an icon for your app catalog. This icon appears on the home screen of the device.</p> <p>If you do not upload an icon, Workspace ONE UEM pushes a default icon to devices.</p>

Customization

Setting	Description
Branding Logo	<p>Upload a logo to brand the app catalog for your organization.</p> <ul style="list-style-type: none"> ■ This logo overrides any logo you set in Groups & Settings > All Settings > System > Branding. ■ If you do not upload a logo for the app catalog, Workspace ONE UEM uses the logo from your System > Branding settings. ■ If you do not configure any branding scheme or logo the System > Branding settings, Workspace ONE UEM uses a default scheme.
Default Filter	<p>Sets the app catalog to open with this filter enabled on the catalog's main page. However, if users need to install featured applications, the app catalog defaults to open with the Featured filter.</p> <p>Users can change the default filter at any time and their selection stays active if they use the app catalog within a 24 hour period. After more than 24 hours of inactivity, the app catalog returns to the set default filter.</p>
Default Sort	<p>Sets the app catalog to open with a configured sorting option enabled.</p> <p>Users can change the default sort at any time and their selection stays active and does not depend on activity.</p>
Pinned Categories	<p>Pins specific categories to the default menu.</p> <p>Users can elect to see more categories.</p>

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Workspace ONE / Catalog / Standalone Catalog

The Standalone Catalog settings page lets you configure various options related to the standalone app catalog.

Many organizations do not need to manage devices for their mobile fleets for various reasons, including possible privacy or legal issues. However, they may need to distribute mobile applications, so Workspace ONE UEM offers the flexibility of deploying the Standalone Catalog.

Users do not have to enroll with Workspace ONE UEM using the Workspace ONE Intelligent Hub, but rather enroll with the Workspace ONE UEM Standalone Catalog. This catalog distributes all application types, public, purchased, internal, and web.

Although end user devices are not enrolled in MDM, you can access a device record in the UEM Console. The device record is for auditing purposes and the status of these devices in the UEM Console displays as **App Catalog Only**.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Standalone Catalog	Enable the Standalone Catalog to prevent users that enroll into the selected App-Catalog-Only-Organization-Group from enrolling into MDM. Configure this setting in the App-Catalog-Only-Organization-Group or in a parent above it.
Allow New User Registration	Enable the Allow New User Registration check box to allow new users to register for access to the Standalone Catalog.
Enable Email Domain Validation	Select the Enable Email Domain Validation option to use specified email domains to validate users when they register to access to the Standalone Catalog. Enter email domains in the Allowed Email Domains field for the standalone MAM users. End users enter their email addresses and a Group ID to enroll with this Standalone Catalog. Workspace ONE UEM matches the domains entered in this field to the domains of MAM-only users.
Catalog Title	Enter a title in the Catalog Title field.
Icon	Upload an image in the Icon field for the Standalone Catalog.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Workspace ONE / App Restrictions

The App Restrictions settings page lets you configure a setting that lets you control which public apps can be installed on devices.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Restricted Mode for Public iOS Applications	Enable this setting to restrict devices to only install assigned public apps from the iTunes App Store. This setting will send a restriction profile that blocks iTunes App Store access on iOS devices in the organization group so you do not have to configure any additional restriction profiles to block app store access.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Workspace ONE / Application Categories

You can define your own application categories to filter applications and books by type or function. Although they are labeled application categories, they apply to Workspace ONE UEM books, as well.

You can create, view, edit, delete, and assign one or more categories for both public and internal applications and books in a selected organization group. The App and Book Catalogs display these categories, allowing end users to browse and filter.

Apps / Workspace ONE / External App Repository

The External App Repository settings page is where you can set up a connection to your own external app repository server.

Host internal applications on your network with an external application repository and manage the applications with the Workspace ONE UEM. The Workspace ONE UEM uses Windows File Share protocols to make externally hosted applications available to user devices. Communication is secure because on-premises deployments must use the Content Gateway for Windows to transfer data from the on-premises network to the Workspace ONE UEM.

Setting	Description
Username	Enter the username for the external app repository.
Password	Enter the password for the external app repository.

Apps / Workspace ONE / Application Removal Protection

The app removal protection feature helps ensure that the system does not remove business-critical applications unless approved by the admin.

Internal applications are often developed to perform enterprise-specific tasks. Their abrupt removal can cause user frustration and halt work. To prevent the removal of important internal applications, the feature holds removal commands according to entered threshold values. Until an admin acts on the held commands, the system does not remove internal applications.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Devices Affected	Enter the maximum amount of devices that can lose a critical application before the loss hinders the work of the enterprise.
Within (minutes)	Enter the maximum amount of minutes that the system sends removal commands before the loss of a critical application hinders devices from performing business tasks.
Email Template	Select an email notification template and make customizations. The system includes the App Remove Limit Reached Notification template, which is specific to app removal protection.
Send Email to	Enter email addresses to receive notifications about held removal commands so that the recipients can take actions in the app removal log.

Apps / Workspace ONE / Catalog / Featured Applications

Use the featured application option to set a few select applications apart from other applications and to highlight specific applications within the AirWatch Catalog for your end users.

Note In past Workspace ONE UEM versions, you could set trending apps and featured categories using the **Featured Apps** page. However, these options are deprecated at this time, but are being worked on for future releases. To highlight categories, you can use the **Pinned Categories** option in the **Catalog** settings.

Supported Platforms and App Types

You can configure Featured Applications for the following platforms:

- Android
 - Internal applications
 - Public applications
- Apple iOS
 - Internal applications
 - Public applications

Configuring Featured Applications

The AirWatch Catalog lists featured apps in the main list of applications. You can feature public and internal applications.

Devices & Users / Apple / VPP Managed Distribution

Use Apple's Managed Distribution system integrated with Workspace ONE UEM to distribute your free and purchased Volume Purchase Program (VPP) applications and books to Apple iOS 7+ devices. The managed distribution model uses service tokens (also called sTokens) to retrieve your VPP contents and distribute them to devices using the UEM console.

Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > VPP Managed Distribution**.

For more information on the settings on this page and how to enroll in the Apple VPP, deploy apps, configure managed distribution, and more, please see the topic called **Volume Purchase Program (VPP)** in the **Integration with Apple Business Manager** documentation.

Setting	Description
Description	<p>Enter your VPP Account ID.</p> <p>Using your VPP Account ID as the description has several advantages:</p> <ul style="list-style-type: none"> ■ Identifies the correct account if you use multiple sTokens. ■ Reminds you the correct account when you renew the sToken. ■ Identifies the correct account to others in your organization who take over managing the VPP account.
SToken Upload	Select Upload to navigate to the sToken on your network.
Country	<p>Select where Workspace ONE UEM should validate the sToken.</p> <p>This value reflects the region from where you bought content and ensures Workspace ONE UEM uploads the correct versions of your purchases.</p> <p>When you sync your licenses, Workspace ONE UEM pulls the correct regional version of the content.</p> <p>If Workspace ONE UEM cannot find the content in the app store from the region entered, Workspace ONE UEM automatically searches the iTunes App Store in the United States.</p>
Automatically Send Invites	<p>Send invitations to all the users immediately after you save the token. This is an invitation to join and register with Apple's VPP, so that users access the terms of use for participating in the program.</p> <p>Use the Message Preview option to review the invitation.</p> <p>Note If your environment includes VPP applications set to the Assignment Type, Auto, then Workspace ONE UEM sends invitations no matter how you configure this option. This behavior facilitates quick access to applications upon enrollment.</p> <p>Workspace ONE UEM automatically sends users of Apple iOS 7.0.3+ an invite command when you enable this option. It does not send them an email message.</p> <p>You do not have to enable this immediately. You can leave it disabled and still upload your token. Return and enable this feature to send invitations to all the enrolled devices whose users have not yet accepted to join the VPP.</p>
Message Template	Select an email template for an email message invitation for Apple iOS devices on Apple iOS 7.0.0 through 7.0.2.

Apps / Workspace ONE / Paid Public Applications

The Paid Public Applications settings page lets you enable the management of paid public iOS apps when using Apple's Volume Purchase Program is not an option.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Management Of Paid Public Application	Enable this setting to upload paid public iOS apps and distribute them in those distribution scenarios where using the VPP is not feasible. Workspace ONE UEM can apply deployment options to offer control over the use of the app.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Container

This Workspace settings page allows you to configure an AirWatch Container application with a different Bundle ID.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Notification	
Apple	Select to set iOS device system preferences.
Android	Select to set Android device system preferences.
Application Type	Leave the application type as System or select Internal to set system preferences. <ul style="list-style-type: none"> ■ System – Download this app type from an app store. ■ Internal– Upload this app type to the UEM console.
Application Name	Provide an app name for Internal applications. Navigate to Apps & Books > Internal List View and scan the list for an app name that matches the app name you entered. This list view only displays internal applications were uploaded with a matching APNs certificate.
Bundle ID	Review the auto-populated field. This Bundle ID matches the application bundle ID that was uploaded internally or selected from the drop-down menu.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Inbox

The Inbox settings page lets you configure options related to the VMware Inbox application.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Application Type	Leave the application type as System or select Internal to set system preferences. <ul style="list-style-type: none"> ■ System – Download this app type from an app store. ■ Internal– Upload this app type to the UEM console.
Application Name	Provide an app name for Internal applications. Navigate to Apps & Books > Internal List View and scan the list for an app name that matches the app name you entered. This list view only displays internal applications were uploaded with a matching APNs certificate.
Bundle ID	Enter the bundle ID of the application.

Setting	Description
Settings and Policies	
Application Profile	<p>Select an application profile to apply SDK functionality to your app.</p> <ul style="list-style-type: none"> ■ Default Allow applications to use the default security policies and settings defined under Apps and Books > Settings > Settings and Policies. ■ Custom Override default settings and apply custom profiles. Custom profiles use the security policies and settings defined under Apps and Books > Settings > Settings and Policies > Profiles.
iOS SDK Profile	<p>Select the corresponding profile from the drop-down menu. This profile applies the default security policies and settings defined under Settings & Policies OR the custom security policies and settings defined under Profiles.</p> <p>This is an optional, advanced management feature. Instructions for configuring default SDK settings are available in the VMware Workspace ONE UEM Mobile Application Management Guide.</p>

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. Inherit only means child OGs are only allowed to inherit these settings. Override only means they override the settings, and Inherit or Override means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Video

The Video settings page lets you configure various settings related to the Workspace ONE UEM Video mobile app.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Settings and Policies	
Application Profile	<p>Select an application profile to apply SDK functionality to your app.</p> <ul style="list-style-type: none"> ■ Default – Allow applications to use the default security policies and settings defined under Apps and Books > Settings > Settings and Policies. ■ Custom – Override default settings and apply custom profiles. Custom profiles use the security policies and settings defined under Apps and Books > Settings > Settings and Policies > Profiles.
iOS SDK	Select the appropriate profile from the drop-down menu that appears when you enable a Custom Application Profile to override default SDK settings.
SDK	Select the appropriate profile from the drop-down menu that appears when you enable a Custom Application Profile to override default SDK settings.
General	
Require MDM Enrollment	Select to require Workspace ONE UEM MDM enrollment for Workspace ONE UEM Video access.
Notification	
Apple	Select to set iOS device system preferences.
Android	Select to set Android device system preferences.

Setting	Description
Application Type	<p>Leave the application type as System or select Internal to set system preferences.</p> <ul style="list-style-type: none"> ■ System – Download this app type from an app store. ■ Internal – Upload this app type to the UEM console.
Application Name	<p>Provide an app name for Internal applications.</p> <p>Navigate to Apps & Books > Internal List View and scan the list for an app name that matches the app name you entered. This list view only displays internal applications were uploaded with a matching APNs certificate.</p>
Bundle ID	<p>Review the auto-populated field. This Bundle ID matches the application bundle ID that was uploaded internally or selected from the drop-down menu.</p>

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Apps / Settings and Policies / Security Policies

The Security Policies page lets you configure options that affect Workspace ONE UEM apps and wrapped apps.

Apps / Settings and Policies / Settings

The Settings and Policies Settings page lets you configure options that affect Workspace ONE UEM apps and wrapped apps.

Apps / Settings and Policies / Profiles

The Settings and Policies > Profiles page lets you create custom app wrapping and SDK profiles that you can assign to your internal apps. Custom settings for profiles offer granular control for specific applications and the ability to override default (security policies) settings. However, they also require separate input and maintenance.

Not all of the settings here apply to both app wrapping profiles and SDK profiles.

Apps / Microsoft Intune® App Protection Policies

You can configure the data loss prevention (DLP) application policies for your Microsoft Intune® App Protection applications in Workspace ONE UEM.

Microsoft Intune® App Protection Policies allow administrators to configure policies to protect Office 365 apps and data using Microsoft's Graph APIs. After you integrate the two systems, you can manage the DLP application policies in the UEM console so that the integration stays current.

Content

5

This section provides information about the Workspace ONE UEM Content settings.

The Workspace ONE UEM Content settings are categorized into the following:

- Applications
- Content Gateway
- Personal Content
- Remote Storage
- User Storage
- Content Viewer
- Advanced

This chapter includes the following topics:

- [Content / Applications / Content Locker Sync](#)
- [Content / Applications / Workspace ONE Content App](#)
- [Content / Content Gateway](#)
- [Content / Personal Content](#)
- [Content / User Storage](#)
- [Content / Remote Storage](#)
- [Content / Content Viewer](#)
- [Content / Advanced / File Extensions](#)
- [Content / Advanced / Onboarding](#)

Content / Applications / Content Locker Sync

The VMware Content Locker Sync settings page lets you configure the various options for using the VMware Content Locker Sync client.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Important VMware Workspace ONE has announced January 3rd, 2020 as the End of Life (EOL) date for Personal Content and its related features.

Table 5-1. VMware Content Locker Sync Settings

Setting	Description
Content Locker Sync	Enable to allow end users to use the VMware Content Locker Sync client.
Client Download	Enable to allow end users to download the VMware Content Locker Sync client to their macOS or Windows 7 devices from the Self-Service Portal.
Require MDM Enrollment	Enable to require MDM enrollment before devices sign in to VMware Content Locker Sync to enforce compliance.
Required Terms of Use	Select the Terms of Use end users must agree to follow before using VMware Content Locker Sync.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Content / Applications / Workspace ONE Content App

The VMware Workspace ONE Content settings page lets you configure the various options for the Workspace ONE Content application.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Settings and Policies

Setting	Description
Application Profile	Set to define the security policies and settings used by this application. Leave as Default and configure the Recommended Default SDK settings to define app behavior using Workspace ONE UEM recommendations. Alternatively, select Custom application settings to override the default SDK settings and configure a unique set off behaviors for the app.
iOS Profile	Select a custom-created SDK profile from the drop-down list.
Android Profile	Select a custom-created SDK profile from the drop-down list.

Setting	Description
Use Legacy Settings and Policies	Only enable legacy settings if directed to do so by a Workspace ONE UEM representative. Legacy settings do not leverage Shared SDK profile settings and should only be implemented in certain edge cases.
Default Authentication Method	Select the authentication method for the applications.
Enable "Keep me signed in"	Enable to allow end users to remain signed in between uses.
Maximum Number of Failed Attempt	Set the number of passcode entry attempts allowed before all data in the Workspace ONE Content will be wiped from a device.
Authentication Grace Period (min)	Enter the time (in minutes) after closing the Workspace ONE Content before reopening the Workspace ONE Content will require users to enter credentials again.
Prevent Compromised Devices	Enable to prevent compromised devices from accessing Workspace ONE Content.
Enable Offline Login Compliance	Enable to allow offline login compliance.
Maximum Number of Offline Logins	Enter the number of offline logins allowed before you have to go online.

General

Setting	Description
Numbers of Days to Keep Content New	Select the number of days recently added documents will be labeled as new in the Workspace ONE Content.
Block Enrollment via Content Locker, Boxer, and Browser	<p>Enable to prevent enrollment through Workspace ONE Content, Workspace ONE Boxer, and Workspace ONE Web.</p> <p>If Workspace ONE Content uses the Workspace ONE SDK for iOS in Objective-C, then MDM enrollment is required for the single-sign on SDK setting to function correctly.</p>
Change Repository Name	Enable to change the repository name in the Root Repository Name field that appears.
Root Repository Name	Enter the new repository name you want to use.
Allow Hyperlinks	Enable to allow end users to open hyperlinks located in documents in the Open Internet Links with field that appears.
Open Internet Links with	Select the application in which to open hyperlinks.
Local Storage	<p>Enable to provide a storage alternative for user content. Local storage saves on the device and doesn't sync with other Personal Content in the cloud.</p> <p>Disable local storage to force all user content to save in a location that syncs with other Personal Content in the cloud.</p>
Upload on Wi-Fi Only	Enable to restrict uploads from Workspace ONE Content to Wi-Fi connections only.

Terms of Use

Setting	Description
Required Terms of Use	Select the Terms of Use end users must accept.

Notification

Setting	Description
Platform	Select the platform for which to configure notification settings.
Application Type	Select to use a System or Internal application.
Application Name	Select the application's name.
Bundle ID	Select the Bundle ID number used to identify the app in the app store.
Badge Count	Select the type of notifications that create app badges.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Content / Content Gateway

The Content Gateway is an enterprise integration component that acts as a secure and effective medium for end users to access corporate content. The Content Gateway settings page is used to configure the Content Gateway component.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Settings	Description
Enable the Content Gateway	Set Enable the Content Gateway to Enabled . You might need to select Override to unlock Content Gateway settings.
Add	Select Add to begin configuring the Content Gateway. You must choose the Installation Type, enter the Content Configuration details and enable the Content SSL Certificate settings.
Installation Type	Select the Operating System for the Content Gateway server.

Settings	Description
Content Configuration	<ul style="list-style-type: none"> ■ Configuration Type - Select either Basic or Relay. Basic is the endpoint configuration with no relay component. Relay is the Endpoint configuration with a relay component. ■ Name- Provide a unique name used to select this Content Gateway instance when attaching it to a Content Repository, Repository Template, or RFS Node. ■ Content Gateway Relay Address - If implementing a relay configuration, enter the URL used to access the Content Gateway Relay from the Internet. ■ Content Gateway Relay Port- If implementing a relay configuration, enter the relay server port. ■ Content Gateway Endpoint Address - Enter the host name of the Content Gateway endpoint. The Public SSL certificate bound on the configured port must be valid for this entry. ■ Content Gateway Endpoint Port - Enter the endpoint server port.
Content SSL Certificate	<ul style="list-style-type: none"> ■ Public SSL Certificate (required for Linux requirements) - If necessary, upload a PKCS12 (.pfx) certificate file with a full chain for the Content Gateway Installer to bind to the port. The full chain includes a password, server certificate, intermediates, root certificate, and a private key. Requirements vary by platform and SSL configuration. ■ Ignore SSL Errors (not recommended) - If using a self-signed certificate, consider enabling this feature. If enabled, Content Gateway ignores certificate trust errors and certificate name mismatches.

Content / Personal Content

The Personal Content settings pages lets you configure the various options for personal content.

Important VMware Workspace ONE has announced January 3rd, 2020 as the End of Life (EOL) date for Personal Content and its related features.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Storage Allocation

Setting	Description
Storage Quota	<p>Divide the allocated storage between the Workspace ONE UEM Managed and Personal Content repositories, dedicating an amount of the available storage to Personal Content.</p> <p>By default, all available storage gets dedicated to Personal Content, indicated by the far-right position of the slider.</p>
User Quota	Set the maximum amount of storage any one user can consume, in MB. This quota applies to users in the same Organizational Group hierarchy as Storage Quota.
User Group Quota(s)	Select Add New and configure storage exceptions on a user group basis.

Shared Links

Setting	Description
Link Sharing	Enable link sharing of documents.
Auto Expire Days	Enable and fill in a numerical value to specify the number of Days links remain available for sharing. Disable to leave the option open for end users to configure when they share their links.
Auto Expire Downloads	Enable and input a numerical value to set the maximum number of Downloads before the link expires. Disable to leave the option open for end users to configure when they share their links.
Require Password Protection	Enable and set the Minimum Length in characters and the Complexity of the password. Disable to leave the option open for end users to configure when they share their links.

Shared Folders

Setting	Description
Folder Sharing	Enable to provide end users with the option to share folders with other users.
Share with User Groups	Enable to provide end users with the option to share folders with entire user groups in lieu of manually listing each user they want to share their folder with.
Available Sharing Roles	Set the access privilege role for those that end users share a folder with. See the Sharing Roles matrix below, for an overview of sharing roles and their permissions.
Share with External Users	Enable to allow end users to share folders with external users.
Available Sharing Roles	Set the role for those that end users share their folder with. See the Sharing Roles matrix below, for an overview of sharing roles and their permissions.
User Quota	Leave the quota at 0 to have all external user uploads count against the folder sharer's quota. Set a quota to give external users dedicated space for uploads.

Sharing Roles

The matrix below displays the available roles and their permissions available for selection when you enable user group and external user sharing. These permissions apply to the user group or external user that an end-user shares a folder with.

Table 5-2. Permissions by Role

	Owner	Co-Owner	Editor	Reader	Viewer
View File and Folders	✓	✓	✓	✓	✓
Download Files to Computer	✓	✓	✓	✓	
Add Comments to Files	✓	✓	✓	✓	✓
Upload Files to Folder	✓	✓	✓		
Delete Files or Sub-folders	✓	✓	✓		
Edit Files	✓	✓	✓		
View Other Folder Collaborators	✓	✓	✓		

Table 5-2. Permissions by Role (continued)

	Owner	Co-Owner	Editor	Reader	Viewer
View Other Collaborators Activity in Feed	✓	✓	✓	✓	
Modify Sharing of Folder	✓	✓			
Generate Shared Links to Files	✓				
Transfer Folder Ownership	✓				

Email Notification

Setting	Description
Email Notifications	Enable to alert users through email when a folder is shared with them.

Data Loss Prevention

Setting	Description
Allow Open in Email	Enable to allow content to open in emails. Disable for maximum security.
Allow Open in Third Party Apps	Enable to open personal content in other applications. You can set a list of approved apps in the SDK Profile. Disabling this option also disables the end user's permission to print the PDF documents from the iOS VMware Workspace ONE Content. Disable for maximum security.
Allow Printing	Enable iOS devices to print personal content PDFs using AirPrint. Printing is supported only if Allow Open in Third Party Apps is enabled. Disable for maximum security.
Watermark	Enable to apply a dynamic watermark to the files rendered in the HTML5 Viewer. By default, the user's email is applied as the file's watermark. You can reconfigure the watermark text in the SDK.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Content / User Storage

The User Storage settings page lets you edit and remove the user content storage quotas. View the available content using the Summary overview available on the main screen.

Select the **Edit** icon to override User Storage on an individual level. This takes precedence over organization group or user group storage quota configurations. On selecting a storage quota, the **Delete** button becomes visible. Select **Delete** to enter a pin and delete a user's content. A pin configuration is in place to prevent the administrators from deleting the user content.

Content / Remote Storage

The Remote Storage settings page lets you configure the various options for remote file storage of personal content.

Important VMware Workspace ONE has announced January 3rd, 2020 as the End of Life (EOL) date for Personal Content and its related features.

Standalone RFS

SaaS	On-Premise
Use RFS instead of the cloud-based Workspace ONE Database to store your organization's personal content. Benefits include:	Use RFS instead of the Workspace ONE Server to store your organization's personal content. Benefits include:
<ul style="list-style-type: none"> ■ Addressing security concerns about storing private information in the cloud. ■ Meeting requirements to utilize the Content Rendering Engine. 	<ul style="list-style-type: none"> ■ Meeting requirements to utilize the Content Rendering Engine. ■ Leveraging existing storage infrastructure. ■ Complying with physical data storage regulatory requirements. ■ Minimizing Internet bound bandwidth consumption.

RFS with CRE

- Rendering of personal content files store in RFS in an HTML5 enabled browser.
- Sharing content without losing control of data.
- Protecting sensitive documents with a dynamic watermark.
- Enforcing "View Only" restrictions for content shared with external parties.
- Improving usability.

Content / Content Viewer

The Content Viewer settings pages lets you configure the various options for the Content Viewer.

Prerequisites

If you do not have an RFS instance set up, select **Configure**.

If you previously installed an RFS instance, select **Add**.

Procedure

- 1 Navigate to **Content > Settings > Content Viewer**, at a Customer level Organization Group.
- 2 Select **Configure** if configuring the first CRE instance.
After the first instance, the option switches to **Add**.
- 3 On the **Assignment** screen, select an **RFS Node** from the same data-center or network as CRE to have content rendered in the SSP. Select **Next**.

Limit one CRE instance per RFS node.

- 4 Configure the fields on the **Details** screen. Select **Next**.

Setting	Description
Name	Provide a name for the content viewer. This name displays in the UEM Console.
CRE URL	Provide the externally accessible URL for the CRE you set up on your server.

- 5 Assign a **Public SSL Certificate** on the **Authentication** screen to establish trust between RFS and the Content Viewer. Select **Next**.
- 6 Select the **Edit** icon from the actions menu for the CRE node.
- 7 Select the **Advanced** tab.
- Copy and record the **Client ID**.
 - Select **Generate PEM**. Copy and paste the text into a text editor, saving it as a .pem file.
Save the text as **CreClientCertificate.pem**.
- 8 Review the **Summary** screen. Select **Save** after reviewing the newly configured settings.
- 9 Select **Download** under the **Installer** column and follow the prompts.
- 10 Use the manual utility to upload the SSL certificate to the RFS Tokens server selected during configuration.

Content / Advanced / File Extensions

The File Type settings page lets you configure the various options for supported file types for personal content.

Important VMware Workspace ONE has announced January 3rd, 2020 as the End of Life (EOL) date for Personal Content and its related features.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Allowed File Extensions	Specify the file type allowed for upload and repository sync.
Apply Restrictions to Personal Content	Set to Yes to apply restrictions to personal content.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Content / Advanced / Onboarding

The Onboarding settings page lets you configure the various options for required content in the VMware Content Locker.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Onboarding	Enable to lock the end user's iOS device in the VMware Content Locker application until the end user has completed all required content.
Administrative Unlock Code	Enter the code that allows administrators to unlock iOS devices that are locked in Onboarding.
Entrance Message	<p>Enable to display a message to users when signing in to VMware Content Locker for the first time when onboarding is enabled.</p> <ul style="list-style-type: none"> ■ Message Text – Enter the message to display as an entrance message.
Exit Message	<p>Enable to display a message when exiting onboarding mode.</p> <ul style="list-style-type: none"> ■ Message Text – Enter the message to display as an exit message.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

This section provides information about Workspace ONE UEMEmail settings.

The Workspace ONE UEM Email settings are categorized into the following:

- Configuration
- Email Notification

This chapter includes the following topics:

- [Email / Configuration](#)
- [Email / Email Notification](#)

Email / Configuration

The Email Configuration page lets you configure the various options for using Workspace ONE UEM Mobile Email Management.

Mobile Email Management configuration uses a wizard to help you set up email for devices.

Email / Email Notification

The Email Notification page provides access to the Email Notification Service installer. The ENS provides email notification for AirWatch Inbox and VMware Boxer applications.

Select the **Enable Email Notification** check box to enable the email notification for AirWatch Inbox or VMware Boxer mail clients.

General

- **Cloud Service URL** - Enter the AirWatch cloud notification service URL. This is the URL to which the Email Notification Service (ENS) server sends notifications.

On selecting **Save**, the **Download Email Notification Installer** link appears on the screen.

Select the **Download Email Notification Installer** link, create a password for Email Notification Certificate, and download the installer to the local folder.

Advanced

View the generated and API key on the advanced page.

- **Regenerate Certificates** - Select this to generate a new certificate.
- **Regenerate API Key** - Select this to generate a new API key.

Telecom

7

This section provides information about the Workspace ONE UEM Telecom settings.

The Workspace ONE UEM Telecom settings are categorized into the following:

- General
- Jasper Integration

This chapter includes the following topics:

- [Telecom / General](#)
- [Telecom / Jasper Integration](#)

Telecom / General

The Telecom General page displays the current Telecom configuration and lets you change the various options available through Telecom Management.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.
- **Enable Telecom Management** – Enable to use the Workspace ONE UEM Telecom Management system and configure the various options.

Changing the Pooled Plan Usage ranges in the System Settings menu only configures how users' plan consumption is displayed on the Telecom Dashboard, and is for reference purposes only. Data presented and configured in the UEM console may not reflect actual carrier billing.

Workspace ONE UEM default values for Usage Ranges are:

Range	Calls	Data	Messages
Very Low	0 to 499 minutes	0 up to 1 GB	0 to 499 messages
Low	500 to 999 minutes	1 up to 2 GB	500 to 999 messages
Medium	1000 to 1499 minutes	2 up to 3 GB	1000 to 1499 messages
High	1500 to 1999 minutes	3 up to 4 GB	1500 to 1999 messages
Very High	2000+ minutes	4+ GB	2000+ messages

Apple iOS

- **Change These Settings** – Selecting this option opens [Devices & Users / Apple / Apple iOS / Hub Settings](#).

Android

- **Change These Settings** – Selecting this option opens [Devices & Users / Android / Hub Settings](#).

Privacy

- **Change These Settings** – Selecting this opens [Devices & Users / General / Privacy](#).
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Telecom / Jasper Integration

The Telecom Jasper Integration page lets you connect your Jasper account to manage SIM cards through Workspace ONE UEM.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Setting	Description
Jasper Integration	Enable to use the Jasper Integration system to configure the user settings.
Username	Enter the username associated with your Jasper account.
Password	Enter the password associated with your Jasper account.
API Key	Enter your API generated from your Jasper console.
API URL	Enter the API URL associated with your Jasper account.

- **Test Connection** – Select to check if there is connectivity between the Workspace ONE UEM console and the Jasper account.
- **Clear Account** – Select to clear all the Jasper Integration settings.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. Inherit only means child OGs are only allowed to inherit these settings. Override only means they override the settings, and Inherit or Override means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

This section provides information about the Workspace ONE UEM Admin settings.

The Workspace ONE UEM Admin settings can be categorized into the following:

- Console Security
- Data Purging
- Cloud Services
- Diagnostics
- Events
- Licenses
- Monitoring
- Scheduler
- Settings Management
- Storage
- Troubleshooting
- Content Delivery Settings
- Policy Engine Settings
- Data Samples
- Custom Attribute Settings
- Product Provisioning
- UEIP

Most of the following settings pages are applicable to on-premises customers only. If you are a SaaS customer you may not see some or all of these pages.

This chapter includes the following topics:

- [Admin / Console Security / General](#)
- [Admin / Console Security / Passwords](#)
- [Admin / Console Security / Session Management](#)

- [Admin / Data Purging](#)
- [Admin / Cloud Services](#)
- [Admin / Diagnostics / Logging](#)
- [Admin / Diagnostics / System Health](#)
- [Admin / Events](#)
- [Admin / Licenses / Device](#)
- [Admin / Monitoring](#)
- [Admin / Scheduler](#)
- [Admin / Settings Management / Settings Audit](#)
- [Admin / Settings Management / Settings Summary](#)
- [Admin / Settings Management / Settings Comparison](#)
- [Admin / Storage](#)
- [Admin / Troubleshooting / Web Console Log](#)
- [Admin / Troubleshooting / Directory Connectivity Tool](#)
- [Admin / Troubleshooting / SCEP Certificate Tool](#)
- [Admin / Content Delivery Settings](#)
- [Admin / Policy Engine Settings](#)
- [Admin / Data Samples](#)
- [Admin / Custom Attribute Settings](#)
- [Admin / Product Provisioning](#)
- [Admin / Product Improvement Programs](#)

Admin / Console Security / General

Note The settings on this page can only be configured at the Global level.

The Console Security – General settings page lets you enforce some additional security surrounding logins to your Workspace ONE UEM console environment. When the number of failed logins exceeds a specific amount, you can enforce High Alert Mode.

Strict Mode

Setting	Description
Strict Mode Active	Select this option to enforce High Alert mode with preset parameters.

High Alert Mode

Setting	Description
Active	Select this option to enable High Alert Mode when the following parameters are met.
Allowed Failed Logins	Enter the number of allowed failed login attempts. Any failed attempts exceeding this number triggers logout.
Duration (mins)	Enter the amount of time in minutes that the is locked out.

Admin / Console Security / Passwords

The Password settings page lets you configure settings related to administrator passwords for the Workspace ONE Unified Endpoint Management (UEM) console.

Note Password policy settings can only be configured at the Global organization group.

Password Policy

The following apply to admin accounts you created in Workspace ONE UEM.

Setting	Description
Enforced password history	Select how many passwords the UEM console remembers and prevents the administrator from reusing.
Password Expiration Period (days)	Select the amount of time in days before a password expires.
Minimum password length	Select the minimum length a password can be.
Password complexity level	Select the complexity a password must have.
Maximum invalid login attempts	Select the maximum number of invalid login attempts (maximum of 10) before logout.
Required Password Recovery Questions	Select how many password recovery questions to require admins to have.
Custom Password Recovery Questions	Select whether to allow custom password recovery questions.

Password Recovery Questions

Setting	Description
Active	Determine whether certain questions are available (green) or unavailable (red) as password recovery selections.

Admin / Console Security / Session Management

The Session Management settings page lets you configure settings related to administrator sessions (through different computers or browsers) within the Workspace ONE UEM console.

Note The settings on this page can only be configured at the Global level.

Setting	Description
Forced Session Timeout	Enter the number of minutes an active session lasts before an admin is automatically logged out. A zero entry means forced session timeout is disabled. The default value is 1440 minutes (24 hours).
Idle Session Timeout	Enter the number of minutes an active session can be idle (not interacting with the console) before an admin is automatically logged out. A zero entry means the idle session timeout is disabled. The default value is 240 minutes. SaaS customers are limited to a 60 minute Idle Session Timeout setting due to the load balancer persistence setting.
Allow Multiple Sessions	Enable to allow multiple open sessions, such as in other browsers or on other computers.
Allow IP Address Change	Enable to allow a logged-in admin's IP address to change during a session and remain logged in.
OAuth Token Validity	Enter the number of seconds that an OAuth access token remains valid. A zero entry means the OAuth Token always remains valid. The default value is 3600 seconds (1 hour).

Admin / Data Purging

The Data Purging settings page lets you set a schedule for how frequently data is purged from the Workspace ONE UEM database.

Select the **Edit** icon for any of the rows to configure the frequency with which its data will be purged.

Admin / Cloud Services

The Cloud Services page is where you can enable various Workspace ONE UEM cloud services, such as autodiscovery for enrollment and app wrapping for internal applications.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

AirWatch ID

Setting	Description
Auto Mode	Select AirWatch ID .
Auto Discovery AirWatch ID	Enter your AirWatch ID , or select the hyperlink to register.
HMAC Token	Generate your HMAC Token .

Cloud Services

Setting	Description
Auto Discovery Enabled	<p>– Select to enable this cloud service for autodiscovery enrollment.</p> <p>In order for your on-premises deployment to communicate with the Workspace ONE UEM autodiscovery service to authenticate the HMAC token used for wrapping, you must meet the applicable network requirements.</p>
Auto Discovery Certificate Pinning Enabled	<p>This option is available only when Auto Discovery is enabled. You can upload your own certificate and pin it to the auto discovery function.</p> <p>Select Add a certificate and the settings Name and Certificate display. Enter the name of the certificate you want to upload, select the Upload button, and choose the cert located on your device.</p>
App Wrapping Secure Communication Enabled	<p>This option is for customers who want to host their own app wrapping instances in their own network. Leave this option deselected (disabled) unless you know what it does and have discussed enabling it in your environment with Workspace ONE UEM.</p>

Updates

Setting	Description
Check for Updates	Select this button to check GEM for updates for device OS versions and determine if new ones must be added to the Console UI.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Admin / Diagnostics / Logging

The Logging settings page lets you choose logging levels for the different Workspace ONE UEM components. Based on the selected mode, log files created with two possible levels of detail are generated for each component and saved in the corresponding Workspace ONE UEM server.

- Select **Disabled** to log and save **Error** level messages for each component.
- Select **Enabled** to log and save **Verbose** level messages for each component.

Error level saves only error messages generated to and from the component selected. Verbose level saves every interaction to and from the selected component.

Targeted Logging

You can enable Targeted logging on a per device basis, logging all interactions between the device and Workspace ONE UEM systems.

Setting	Description
Organization Group(s)	Select the organization group(s) where the device(s) reside(s).
Device ID(s)	Enter the device ID(s) for which you want to enable targeted logging. Use commas to separate multiple device IDs.
File Storage Impersonation Enabled	Enable if you are using a file storage server to store these targeted logs and enter the appropriate authentication credentials.
File Path	Enter the path and filename of the LOG file where you would like the data saved.
File Storage Impersonation User Name	This option appears only when File Storage Impersonation Enabled is checked. Enter the username of the storage server where you targeted logs are saved.
File Storage Impersonation Password	This option appears only when File Storage Impersonation Enabled is checked. Enter the corresponding password of the username of the storage server where you targeted logs are saved.
Test Connection (button)	Select this button to test the connection. It tests various possible scenarios which the logging process uses and makes sure it is working as expected.

Note An alternative to entering the Device ID above is to navigate to **Devices > List View**, select a device you want to target, select the **More** drop-down on the device details page, then select **Targeted Logging** and select **Create New Log**.

Admin / Diagnostics / System Health

The System Health settings page lets you monitor the status of various Workspace ONE UEM components, including SEG, VMware Enterprise Systems Connector, and VMware Tunnel.

From this page you can select a component and optionally restart services, view its status, see its event log, and so on.

Admin / Events

The Events settings page lets you view related Console and Device events and their severity and set their log levels.

- **Event Settings** – Select this option to set the log level for Device and Console events. Events that meet the selected levels and above for both Device and Console will be captured and stored by the Workspace ONE UEM database and displayed in the Workspace ONE UEM console on the **Hub > Reports & Analytics > Events > Device Events** and **Hub > Reports & Analytics > Events > Console Events** pages.

Admin / Licenses / Device

The Licenses settings page displays SKU information for each organization group, including the type of licenses, how many were purchased, how many are in use, and when they will expire.

Admin / Monitoring

Configure this page to determine which tools can monitor whether the application server(s) are up. These can include the Admin Console, Device Services, Device Management, and Self-Service Portal. By default any load balancer or monitoring tool can perform this monitoring. For security purposes you can control this monitoring by IP address.

For example, you can set up a load balancer to detect if a given application server is up. The Admin Monitoring settings page lets you whitelist certain IP addresses that can access this page. By default, any IP address is allowed if no IP addresses are defined.

Note The settings on this page can only be configured at the Global level.

Admin / Scheduler

The Scheduler settings page lets you view the Workspace ONE UEM console scheduler tasks and configure the scheduler by setting the frequency with which they occur. You can also disable individual tasks.

Scheduler Task	Description
Admin Password Expiry Notification	Determines how many days before an admin password expires to send an email notification.
Android Enterprise Migration Batch Release Job	During Android (Legacy) migration to Android Enterprise, this task sends commands for the first batch size (300) of devices instantly. After the first 300 devices, the remaining devices will receive the command at the determined intervals. The default interval is 15 minutes.
Android Work Google Device Id Validation Job	Upon enrollment into Android, the server waits for a Google generated deviceID, so that it can initiate the application assignment and push. There are a few minutes delay in getting this ID and this scheduler checks whether any new enrolled device has the ID updated and if yes, start the application sync process.
App EULA Update Notification	Accounts for all devices for which App EULA acceptance is pending and sends notifications. Once final notification is sent, app is removed from the device.
Auto Renew Expiring Profile	Checks for certificates that expired within a renewal grace period configured on Certificate Authority and renews them.
Auto-rotate Google Password	Handles password provisioning and purging for integration with Google Sync.
BitLocker Recovery Key Rotation Job	Rotates the BitLocker admin recovery key based on the values configured in the profile.
Command Publish Batch Job	
Console Notifications	Checks to see if any new notifications must be added to an admin's notification list (for example, APNs expiration notification). These notifications appear in the admin console and are emailed to the admins.
Device Based VPP Apps to Track Update	Checks which VPP applications at an organization group have device-based licensing and auto update enabled. This adds or removes apps from the list used by the VPP auto update scheduler job.
Device Enrollment Program Update	Initiates sync command from Apple to send the added and removed devices for a DEP token at a given OG to update our records.

Scheduler Task	Description
Email Password Removal	Removes Google password generated for email from Workspace ONE UEM database.
File Encryption Migration	Encrypts or decrypts the content stored in the file storage based on the settings in All Settings > Admin > Storage.
Hub Package Process Repository	Watches the package repository directory for WinMo Hub packages and pulls them in to the database.
Install Application On Demand	Triggers install of Apple VPP applications upon VPP invite acceptance and triggers install of failed-eligible Apple VPP applications.
List View Export	Checks if an export is requested by an admin for the device or user list view. If it has, it schedules a background job to run asynchronously. Once that background job is completed, the list view export is available for download.
MDM Application List Sample	Collects the status of applications that are marked as 'MDM apps' from all the devices. Applicable only for iOS apps and devices. Scheduler is turned off by default and is enabled only for customers who request the functionality.
MDM License Count Update	Checks device enrollment counts and updates the customer's license counts. Used to track product usage.
P2P license true-up with vendor	Identifies all the peer distribution server licenses that are about to expire, renews the licenses by communicating with the Adaptiva cloud licensing service and distributes the renewed license key to the peer distribution server.
Peer Distribution Software Notification Job	Identifies all the Peer Distribution servers that do not have the latest version installed and notifies the administrator to update.
Profile Publish Batch Job	Profile publishes for CA and Tunnel profile queues the install profile command in held status is by Profile Publish Batch Job in batches. Selects a batch and batch size, based on the settings configured in the UEM Console (under Settings > Installation > Performance Tuning for on-premise environments).
Purge Marked For Delete	This job deletes repo(s)/folder(s)/file(s) under a repository that is marked for deletion.
Query Feedback Service	Checks Apple's Feedback Service for statuses and causes of failed APNs commands.
Re-queue Device Commands	Applicable only for Windows devices. Identifies devices with failed application installs and re-tries installation. The number of re-try attempts and the interval for the next attempt are identified from the performance tuning settings 'Max re-try attempts for failed app install' and 'Failed Application Install Retry Interval' respectively.
Run Compliance Engine	The scheduler job evaluates compliance in scenarios where: <ul style="list-style-type: none"> ■ Compliance policy is created Post-enrollment. ■ Any subsequent changes are made to the compliance policy. ■ Any changes made to smart group ■ Device moves organization groups ■ Changes made to app groups ■ Certain Telecom based compliance policies are enabled ■ Apple Templates are used
S/MIME Certificate Cleanup	Checks for all SMIME certificates that have completed their retention period and purges them.

Scheduler Task	Description
Scheduled Application Batch Release	Used to release internal application install commands created and held by 'Scheduled Application Publish' job. Selects queued application batch (roundrobin). Calculates device list using configured 'Batch Size' text box of performance tuning section. Releases install commands for batch.
Scheduled Application Publish	Used to trigger the installation and removal of internal applications based on newly effective assignments. Creates held batch of install commands. Creates remove commands for the immediate release.
Send Apps to App Scan Vendor	Send a unique list of applications installed across entire device fleet to the configured app scan vendor.
Send VPP Invites and Apps	Checks for users assigned user-based VPP apps and either sends email or device notifications inviting users or devices to participate in user-based licenses of the Volume Purchase Program.
Server Action Task	Handles Time Schedule profiles. The job runs at configured intervals and takes action of Install or Remove profile as per the time span configured for Time schedule profiles.
Staged Command Data Processing Job	Used to schedule the processing of bulk commands from the Device List View page.
Sync Chrome OS Devices	Retrieves new Chrome OS enrollments from Google and creates a corresponding device record in Workspace ONE UEM.
Sync Directory Groups	Queries the directory to grab all members of synchronized directory groups. Stores users who are part of the group in the UserGroupEnrollmentUserMapSync table. Compares those users by Distinguished Name (DN) or other unique attribute in the UserGroupEnrollmentUserMapSync table to the Mobilemanagement.EnrollmentUser table. If group is configured with add missing users enabled and User does not exist with that DN, user details are pulled from the AD using user ExternalID and stored in the Mobilemanagement.EnrollmentUser table.
Sync Directory User and Admin Attributes	Queries the directory to sync user attributes based on eternalID.
Sync External Content	Syncs admin repo metadata for all the repositories where admin user credentials are set in the MCM console.
Sync MEM Device Resource ID Job	Syncs Google device records with Workspace ONE UEM for approving new enrollments / mobile mail configurations
Telecom Assign Plans/ Roll-up Usage	Calculate usage limits for devices whose Admin has enabled Telecom tracking. Necessary to run reports, populate dashboard, and have the accurate list-view for Telecom.
Temporary Session Key Clean Up	Clears temporary encryption keys used to encrypt the admin provided passphrase in a downloaded configuration file. The key is removed from the database so that it is impossible to retrieve the passphrase from the configuration file after the 48-hour key rotation window has passed.
VPP Auto Update	Checks iTunes for latest version of VPP applications from the list created by Device Based VPP Apps to Track Update job. Each app is checked once every 24 hours. If an update is available, the job kicks off the update command to assigned devices.
VPP Revoke Licenses	Checks for users with associated licenses but no corresponding assigned application. It then issues a revoke command of the license from the user to disassociate it from the license so it can be reused.

Scheduler Task	Description
Workflow Service	Used with the App store restriction, if the restriction is enabled then only one app workflow is active at a time. If there is any issue with the application installation, it deletes in 15 minutes and next one starts.
Purge Job	<p>Removes orphan application blobs from the file storage, and CDN origin server if CDN is configured.</p> <p>Removes expired SDK application log files from the database. By default, the application log files expire every 14 days.</p> <p>Moves any application binary blobs to the file storage from the database if the file storage is configured.</p> <p>Moves non-expired SDK application log files from the database to file storage, if the file storage is configured.</p> <p>Global OG data does not get impacted with respect to the changes made to the blob purge. By default, the scheduler triggers every 24 hours and can either handle 2 GB of data from the database or actively perform tasks for 2 hours.</p>

Admin / Settings Management / Settings Audit

The Settings Audit page lets you enable the settings audit feature, which lists what settings have recently changed, by whom, and when for audit purposes.

Admin / Settings Management / Settings Summary

The Settings Summary page lists all of your environment's Workspace ONE UEM console settings values so you do not have to manually check your database for the values.

Admin / Settings Management / Settings Comparison

The Settings Comparison page lets you compare settings across different organization groups.

As an Administrator, you might find it useful to compare the settings of one organization group (OG) to another. The following are available when you compare OG settings.

- Upload XML files containing the OG settings from different Workspace ONE UEM software versions.
- Eliminate the possibility of a difference in configuration causing problems during version migration.
- Filter the comparison results, allowing you to display only the settings you are interested in comparing.
- Search for a single setting by name with the search function.

Admin / Storage

The Admin Storage settings page lets you set the maximum file capacity for apps and content.

The **Type** drop-down menu allows you to view the capacity, usage and percentage for each organization group. The **Edit Defaults** icon allows you to change these settings.

Admin / Troubleshooting / Web Console Log

The Web Console Log settings page displays the latest Console log file for downloading so you do not have to manually log into the Console server to access it.

Note The settings on this page can only be configured at the Global level.

Admin / Troubleshooting / Directory Connectivity Tool

The Directory Connectivity Tool lets you enter details about a directory service and test connectivity with the Workspace ONE UEM console. Using this page, you do not need to go through the integration steps necessary to configure directory service integration with Workspace ONE UEM. You can simply enter the details here and test the connection.

Admin / Troubleshooting / SCEP Certificate Tool

The SCEP Certificate Tool lets you test connectivity between your SCEP endpoint and Workspace ONE UEM. Select a configured CA and Request Template from the drop-down lists.

Admin / Content Delivery Settings

The Content Delivery Settings page lets you configure the options for using relay servers as part of your product provisioning solution.

Setting	Description
Packages Cache	Enter the file path on the Workspace ONE UEM application server where products are expanded and prepared for delivery to relay servers.
Relay Server Cache	Enter the file path on the Workspace ONE UEM application server for the working directory for the relay servers.
Temp Cache	Enter the file path for the working directory of the content delivery service.
Minimum Threads	Enter the minimum number of threads available for the content delivery service to communicate with relay servers. If there are more relay servers selected than threads available, then only the number of relay servers as there are threads available contact at once. As a thread completes the operation for the relay server, it moves on to another server.
Maximum Threads	Enter the maximum number of threads available for the content delivery service to communicate with relay servers. If there are more relay servers selected than threads available, then the content delivery service spins up extra threads until it meets the maximum amount. Only the number of relay servers as there are threads available contact at once. As a thread completes the operation for the relay server, it moves on to another server.
Timer Interval	Enter the time between the content delivery service searches for work in the queue.
Maximum FTP Retries	Enter the maximum number of attempts the policy engine attempts to send content to the relay servers before stopping attempts. Once the specified number of attempts have failed for a device, no more attempts will be made for that device until the next time the device checks in.
Pull Max Tries	Enter the maximum number of attempts the pull service attempts.

Setting	Description
Pull Max Connections	Enter the maximum number of simultaneous connections from individual pull servers the Workspace ONE UEM pull service end point services.
Bundle Cache	Enter the path on the Workspace ONE UEM application server where staging packages are expanded and prepared for delivery to relay servers.
File Sources Include Https	Enable to include the Workspace ONE UEM https file handler in the list of file sources for product provisioning. If this is not enabled, only relay servers are considered.
Support Fast Track	Enable to support fast tracking with the policy engine. This means that the policy engine looks at the queue and puts any fast track items at the top of the list.
Failed Relay Server Retry Time	Enter how often, in minutes, the content delivery service processes content service items for a relay server in an error state.

Admin / Policy Engine Settings

The Policy Engine Settings page contains settings related to the policy service of product provisioning. In general, the settings on this page should not be altered unless you know what they do and have discussed it with a Workspace ONE UEM representative. Altering them could adversely affect your environment.

Setting	Description
Minimum Threads	<p>Enter the minimum number of threads the system keeps alive to service work items from the in-memory queue.</p> <p>If there are more work items than threads available, then only the number of work items as there are threads available will make contact at once.</p> <p>As a thread completes the operation for the work item, it will move on to another device.</p>
Maximum Threads	<p>Enter the maximum number of threads the system spawns to service work items from the in-memory queue.</p> <p>If there are more work items selected than threads available, then the policy engine will spin up additional threads until it meets this maximum amount. Only the number of devices as there are threads available will contact at once.</p> <p>As a thread completes the operation for the work item, the system allows it to decay (provided there is no more work in the in-memory queue) down to the minimum threads level.</p>
Timer Interval	Enter the time between the policy engine searches for work in the queue.
Queue Batch Size	The Queue Batch Size is the interval the policy engine picks up work items from the database and claims into the in-memory queue. If set to zero, it attempts to claim everything so in a multiple policy engine scenario, it should be set to a non zero value, like 1000, to avoid starving a policy engine.

Admin / Data Samples

The Data Samples settings page lists the data sample types that you have selected to be stored in the database.

Check a data sample to store latest and historic data samples for that data. Uncheck a data sample to only store the latest sample.

Note The settings on this page can only be configured at the Global level.

Admin / Custom Attribute Settings

When custom attribute auditing is enabled through this system settings page, the Workspace ONE UEM console creates a log record any time the value of a custom attribute for a device is changed. The record contains the device ID, attribute ID, original values and new values, and the date/time it was modified.

Access these records through **Device > Custom Attributes – Search > Change Report API**.

Admin / Product Provisioning

The Product Provisioning page is where you can enable Job Statistics logging to record each job action performed as part of product provisioning.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Settings	Description
Enable Job Statistics	Enable to record each action performed in a job for product provisioning. Such statistics include actions such as "Job Received" and "Job Complete."
Display Offline Provisioning	Enable to turn on a button that displays on the Device Details Page under Products. When this button is selected, the Workspace ONE UEM console creates an offline .zip (or a tar.gz file depending on the platform) containing all of the products or product set jobs and components. Download this .zip file for use offline.
Relay Server Content Transfer	Enable this setting to activate relay server at this organization group to transfer product content. Disabled, this setting stops the relay server from transferring product content and the product content must be transferred to the relay server manually outside of Workspace ONE UEM.
Product Deployment Granularity	Enable this setting to allow the administrator to select whether data is transferred through relay servers always per product or by default with the fail-over to the Workspace ONE UEM server.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Admin / Product Improvement Programs

VMware's Product Improvement Programs give you the opportunity to impact the quality and effectiveness of our products. Our programs enable our Research & Development team to test on a

scrubbed version of our customers' production data, which is essential to ensuring our customers' real-world needs are being met.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Settings	Description
Participate in VMware's Product Quality Improvement Program	<p>Select Yes to influence the experience users encounter while interacting with our products. By opting in to this program, you help us to run critical tests utilizing an anonymous and sanitized version of your production data.</p> <p>Your participation is essential to helping our team ensure your experience using our products is always the best it can be.</p> <p>To learn more about this program, see https://resources.workspaceone.com/view/9yfk6r2pzldhjlhrz9.</p>
Participate in VMware's User Experience Improvement Program	<p>Select Yes to contribute technical information related to the performance, configuration, and use of Workspace ONE UEM. Your participation improves and benchmarks our products and services, fixes problems, and help us to advise customers on the usage of our software.</p> <p>The data is used by VMware and its service providers strictly on an aggregated basis.</p>

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Installation

9

This section provides information about the Workspace ONE UEM Installation settings.

All of the following settings pages are applicable to on-premises customers only. If you are a SaaS customer you may not see some or all of these pages.

The Workspace ONE UEM Installation settings are categorized into the following:

- Cache Settings
- File Path
- Installation Checklist
- Maps
- Performance Tuning
- Proxy
- Reports
- Advanced

This chapter includes the following topics:

- [Installation / Memcached Settings](#)
- [Installation / File Path](#)
- [Installation / Installation Checklist](#)
- [Installation / Maps](#)
- [Installation / Performance Tuning](#)
- [Installation / Proxy](#)
- [Installation / Reports](#)
- [Installation / Advanced / Endpoints](#)
- [Installation / Advanced / File Sync](#)
- [Installation / Advanced / Other](#)

Installation / Memcached Settings

With the Memcached settings, on-premises customers can configure Memcached server nodes.

Memcached is a distributed data caching application available for use with Workspace ONE UEM environments that reduces the workload on the Workspace ONE UEM database. It replaces the previous caching solution, AW Cache, and is intended for deployments of more than 5,000 devices. Once enabled in the Workspace ONE UEM console, Memcached begins storing system setting values and organization group tree information as they are accessed in the Console. When a request for data is sent, Workspace ONE UEM automatically checks for the results stored in memory by Memcached before checking the database, thereby reducing the database workload. If this fails, result data is then retrieved from the database and stored in Memcached for future queries. As new values are added and existing values are changed, they are written to both Memcached and the database. Note that all key/values in Memcached expire after 24 hours.

For more information about the implementation for your on-premises deployment, contact Workspace ONE UEM.

Installation / File Path

The File Paths settings page contains predefined values and you should not change them unless instructed to do so by Workspace ONE UEM. These files paths connect Workspace ONE UEM to specific files and folders used by Workspace ONE UEM services.

File Storage can also be configured on this page, which lets you access apps and content from a file storage server instead of the database to improve performance. Enter the file server details and credentials for the Console to authenticate with the server.

Installation / Installation Checklist

The Installation Checklist settings page contains links to other settings pages that are worth configuring if you have just installed Workspace ONE UEM.

Installation / Maps

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

The Maps settings page lets you view and edit the **MS Bing Key** for communication with their maps API. This is used to display devices on a map within the Workspace ONE UEM console, as well as geofencing policies.

The **Max Locations** setting represents the maximum number of device locations displayed on the Device List View and Location tab of the Device Details pages.

The **Min Distance Between Locations (in ft)** setting represents the minimum distance in feet between consecutive locations reported by the device. If the distance between two reported locations in a row are less than the entered value, then the value is not captured in the console.

- This setting works together with the **Max Device Locations** setting above, which controls how many data points are collected, and the **Min Distance Between Locations** dictates how often they are collected based on the user's movements.
- A value of 0 entered for this setting captures all duplicate locations. So if **Max Device Locations** is set to 100 and **Min Distance Between Locations** is set to 0, then all 100 location data points are taken without regard for the user's change in location, including duplicate locations.
- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Installation / Performance Tuning

The Performance Tuning settings page, found by navigating to **Groups & Settings > All Settings > Installation > Performance Tuning**, contains several options related to action frequencies and thresholds for various UEM console procedures.

Setting	Description
Bulk Publish Commit Frequency	Profiles are pushed to the number of devices entered here per transaction. Minimum value is 1000. Maximum value is 50000. Default value is 40000.
Sample Scheduler Interval (minutes)	This setting determines how often the scheduler pulls a sample from the device, measured in minutes. Minimum value is 1. Maximum value is 1440 (24 hours). Default value is 5.
iOS Device Invites Per Second	This is the number of iOS devices per second that are invited to opt into the VPP program. Minimum value is 4. Maximum value is 100. Default value is 30.
Certificate Profile Publish Frequency	This is the maximum number of certificate profile install commands that can be published at any point in time for your entire environment. Default value is 50.
Certificate Profile Manual Install Threshold	This is the maximum number of certificate profile install commands that can be queued from the dashboard per admin, per profile version. Default value is 100.
Maximum Apple API Calls Per Second (For Invitation of VPP Users)	Specifies the maximum number of calls per second that are made to the Apple VPP servers. Minimum value is 1. Maximum value is 1000. Default value is 30.
Run Real-Time Compliance	
Number of Queue Commands (Max)	<p>This is the maximum number of commands that the queue is allowed to have. Commands are published per the Certificate Profile Publish Frequency until they reach this limit. Once devices consume the commands, more commands are queued up.</p> <p>The value you enter here is multiplied by the 'Certificate Profile Publish Frequency' to get that max number. This number can be increased to improve certificate batching, however, you should consider closely monitoring CA and DS server performance. Default value is 10.</p>

Setting	Description
Certificate Queue Throttling	If the commands added per the Certificate Profile Publish Frequency are not consumed by the devices, the next batch is queued in 30 minutes by default. This time interval can be lowered to improve certificate batching, however, you should consider closely monitoring CA and DS server performance. Default value is 15.
Allow minutes as minimum compliance interval	Enable to create compliance policies and set compliance escalation actions to take place at a minute based interval. Depending on the number of devices enrolled in this environment, the performance of your system might be affected. Please consider these factors before enabling this option.
Batch Size for Internal Application Deployment	This value specifies the number of devices that are included in the batch for internal application deployment. Minimum value is 1. Maximum value is 10000. Default value is 100.
MDM Application List Sample Interval (minutes)	Minimum value 1. Default value 480.
Windows app list sample base poll time (min)	Minimum value 1. Maximum value 1440. Default value 5.
Batch Size for VPP apps license sync	This setting specifies the number of apps included in each batch when they synchronize with the VPP cloud. Minimum value is 1. Maximum value is 250. Default value is 250.
Failed Application Install Retry Interval (Minutes)	This setting specifies how long to wait to attempt a reinstall of a failed application installation. Minimum value is 15. Maximum value is 10000. Default value is 60.
Max retry attempts for failed app install (Windows)	Specifies the maximum number of times to retry a failed installation. Minimum value is 0. Maximum value is 8. Default value is 5.
Device batch size for retrying failed installs	This setting specifies the maximum number of devices included in an attempt to reinstall a failed app installation attempt. Minimum value is 1. Maximum value is 15000. Default value is 10000.
Frequency for device-based VPP app auto updates (hours)	You have the ability to update device-based VPP applications automatically. This setting controls how often, measured in hours, these updates occur. Minimum value is 1. Maximum value is 24. Default value is 1.
App list size to check for app version updates	When the system checks for a new version of an app, this setting specifies the size of the list of apps that are checked. Minimum value is 20. Maximum value is 100. Default value is 20.
Install Certificate Profiles Without Batching on Enrollment	Determines whether or not certificate profile commands are sent in batches. When enabled, batching logic on certificate profile install commands for new enrollments is skipped. When disabled, batching logic on certificate profile install commands for new enrollments is applied.
Sync interval (hours) for VPP license counts at an organization group	This is the minimum amount of time, in hours, that the scheduler spends selecting an organization group to run the Sync License Count. Minimum value is 2. Maximum value is 24. Default value is 6.
Number of organization groups per batch when syncing VPP license counts	This is the number of organization groups the scheduler can select each time it runs the job to synchronize VPP license count. Minimum value is 1. Maximum value is 50. Default value is 10.

Setting	Description
Automatic Delete Factory PPKG	When enabled, the product provisioning package that is uploaded to the device is automatically deleted, saving device storage space. When disabled, the PP package is kept on the device.
Days After Which PPKGs Will Be Deleted	This setting is available only when Automatic Delete Factory PPKG is enabled. This setting determines how many days elapse before the PPKG file is removed from the device. Minimum value is 0 (immediate deletion). Maximum value is 90. Default value is 5.
Product Provisioning AWCM Throttle Rate	Represents the number of AirWatch Cloud Messenger (AWCM) notifications sent per second. Align this throttle rate with the Product Provisioning Command Release Batch Size per the included Product Provisioning Sizing table . Minimum value is 1. Maximum value is 100. Default value is 2.
Product Provisioning Command Release Batch Size	Product provisioning commands are created in a held state. This setting represents the number of commands released from the device command queue per batch release job interval. The scheduler task called "Product Provisioning Batch Release Job" (found in Groups & Settings > All Settings > Admin > Scheduler) controls how often the command queue is released. This setting controls how many commands per interval are released and is aligned with the Product Provisioning AWCM Throttle Rate . Both settings are based on the number of Device Services (DS) servers in your environment, as detailed in the Product Provisioning Sizing table. Minimum value is 1. Maximum value is 10000. Default value is 200.
Apple Profile Installation Batch Size	This value sets the number of profile commands that are added to the command queue per batch. This setting is meant to govern the flow of commands to be processed preventing the procedure from timing out. Minimum value is 300. Maximum value is 1000. Default value is 300.

Product Provisioning Sizing

# of DS servers	AWCM Throttle Rate	Command Release Batch Size
1	2	200
2	4	400
3	6	600
4	8	800
5	10	1000

Installation / Proxy

The Proxy settings page lets you configure various proxy settings if you want to have proxies set up for any of the components listed on this page.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Console Proxy Settings

- **Outbound Connections Go via Proxy** – Lets you set up a proxy for outbound connections from the Console server.

Device Services Proxy Settings

- **Device Services Connections Go via Proxy** – Lets you set up a proxy for outbound connections from the Device Services server.

Socks Proxy Settings

- **APNS go via SOCKS proxy** – Lets you set up a SOCKS proxy to be used for making outbound connections from the Messaging service to send APNS messages.

Google Play Store Proxy Settings

- **Enable** – Lets you set up a proxy to be used for making outbound connections to the Google Play Store.

Installation / Reports

The Reports settings page allows you to enter the reports server details to complete installation of the reports server. It also enables you to configure reports storage. Enable reports storage to store your reports on a dedicated server and increase performance.

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

Reports Storage

Settings	Description
Report Storage Enabled	Enable to use reports and expand all available options.
Report Storage Path	Enter your path in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you created on the server.
Report Storage Caching Enabled	When enabled, a local copy of the files requested for download is stored on the Console server as a cache copy. Subsequent downloads of the same file retrieve it from the Console server as opposed to file storage. If you enable caching, accommodate for the amount of space needed on the server where these files cache.
Report Storage Impersonation Enabled	Enable to add a service account with the correct permissions.
Report Storage Impersonation User Name	Enter the user name of a valid service account with both read, write and modify permissions to the shared storage directory. Displays when Report Storage Impersonation Enabled is enabled.

Settings	Description
Report Storage Impersonation Password	Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when Report Storage Impersonation Enabled is enabled.
Test Connection button	When all required options are completed (denoted by red asterisks), select this button to test connectivity to the reports server.

Installation / Advanced / Endpoints

- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the current organization group's parent OG, while Override enables the settings for editing so you can modify the current OG's settings directly.

The Endpoints settings page displays the information for various device endpoints. Do not change these values unless instructed to do so by Workspace ONE UEM.

- **Child Permission** – Select the available behavior of child organization groups that exist below the currently selected organization group. **Inherit only** means child OGs are only allowed to inherit these settings. **Override only** means they override the settings, and **Inherit or Override** means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Installation / Advanced / File Sync

The File Sync settings page contains several options related to file syncing. You should not alter these values unless instructed to do so by Workspace ONE UEM.

Installation / Advanced / Other

The Installation – Advanced settings page lets you configure options related to the Enrollment and Workspace URLs and SSP Authentication. Except for the one setting mentioned below, you should not alter the settings on this page unless instructed to do so by Workspace ONE UEM.

You can set the default authentication method displayed on the Self-Service Portal depending on your organization's and users' needs.

Note This setting is only accessible at the Global level for on-premises customers.

Configure this setting by navigating to **Groups & Settings > All Settings > Installation > Advanced > Other** and set the **SSP Authentication Type** to:

- **Email** – Prompts users for only their email address if you have set up auto discovery.
- **Legacy** – Prompts users for their Group ID and credentials (username/password).
- **Dedicated** – Prompts users for only their credentials (username/password). This option defaults a single Group ID for single-customer environments.