Self-Service Portal End User Guide

VMware Workspace ONE UEM 2011

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

https://docs.vmware.com/

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

Contents

Self-Service Portal Into Workspace ONE UEM

1

Introduce device end users to the Self-Service Portal (SSP) and empower them to perform basic device management tasks, investigate issues, and fix problems, thus reducing the number of support issues. So while administrators have access to Workspace ONE UEM powered by AirWatch, device end users have the SSP.

Access the Self Service Portal on Devices

You can access the Self-Service Portal (SSP) from your workstations or devices by navigating to **https://<AirWatchEnvironment > /MyDevice**. If you have a device that supports Web Clips or Bookmarks, your administrator can supply these shortcuts enabling you to access the SSP directly.

Self Service Portal (SSP) Customizations

You can alter the default login page background by configuring Branding settings.

Navigate to **Groups & Settings > All Settings > System > Branding** and select the **Upload** button in the **Self-Service Portal Login Page Background** setting. Select a custom background image with a suggested size of 1024x768 pixels.

Product Improvement Program Setting

The Self Service Portal is included in VMware's Product Improvement Program, allowing you to impact the quality and effectiveness of our products. When enabled, this program tests only on usability data, which is essential to ensuring our customers' real-world needs are being met.

You can opt in or opt out of the Product Improvement Program at any time by navigating to **Groups & Settings > All Settings > Admin > Product Improvement Programs**.

To learn more about this program, see https://resources.workspaceone.com/view/9yfkbk6r2pzldhjlhrz9.

Token-Based Security Measures

As a security feature, the following changes have been made for accounts that have enrolled with a token.

- Email Address and Phone Number on both the **Add Device** screen and **Account** screen have been made read-only.
- The View Enrollment Message action has been removed.

This chapter includes the following topics:

My Devices Page of the SSP

The **My Devices** page of the Self Service Portal provides access to detailed information about devices and enables users to perform a wide range of actions in Workspace ONE UEM powered by AirWatch.

The viewable tabs and available actions varies based on device platform. See the applicable platform guide, available on docs.vmware.com.

Select a Language for the SSP

The Self-Service Portal automatically matches the browser default language. However, you can override this default setting by choosing from the **Select Language** drop-down on the login screen.

Log Into the SSP

Log in using the same credentials (**Group ID**, **username** and **password**) used to originally enroll in Workspace ONE UEM.

Change Your Password for the SSP

You may use the **Account** page to change the password associated with your Workspace ONE UEM account. This password will be used for device enrollment and logging into the SSP.

Change your password by selecting the **Account** button located at the top-right of the Self Service Portal screen. The **User Account** page displays allowing you to select the **Change** button next to the **Current Password** field.

Note If a device end user logs into the SSP to change a shared device passcode before it expires, this new passcode adpots the expiration time from the OG associated with the shared device, not the OG the end user is managed from.

For example, assume you have an OG structure with 'Parent' at the top and 'Child' underneath. Assume that the end user account is managed from 'Parent' with a passcode expiration of 90 days. Assume also that the shared device is managed by 'Child' with a passcode expiration of 30 days. In this scenario, when the end user logs into the Self Service Portal and changes the shared device passcode before it expires, the new passcode expiration goes from 90 days (Parent) to 30 days (Child).

The workaround is to ensure that you configure the shared device passcode on the OG the users are managed from.

As the admin, if you change the end user's shared device passcode in the **Add/Edit User** screen from the Workspace ONE UEM console, it correctly adopts the expiration time of the OG the end user is managed from.

Select a Device in the SSP

After logging in to the SSP, the **My Devices** page displays all the devices associated with the account. Each enrolled device appears in its own tab across the top of the **Self Service Portal** page. Select the tab representing the device you want to view and manage.

The device status is listed under the name of the device on the tab. Those statuses include **Discovered**, **Enrolled**, **Pending Enrollment**, **Unenrolled**, and **Enterprise Wipe Pending**.

Add a Device in the SSP

You can add a device directly from the self-service portal.

Procedure

1. Select **Add Device** on the **My Devices** page.
2. Complete the required text boxes: **Friendly Name**, **Platform**, **Device Ownership**, and **Message Type** as applicable.
3. Select **Save** to add the new device to the SSP account.

Results

Note The status of a newly added device sets to "Pending Enrollment" until it is fully enrolled.

Remote Actions in the SSP

The Self-Service Portal of Workspace ONE UEM powered by AirWatch provides a means for end users to use key MDM tools without IT involvement. Provided an administrator allows, end users can run the SSP in a web browser and access key MDM support tools.

Administrators have several remote actions and options for managed devices available to them. However, when devices are employee-owned, those employees might want to access similar management tools for their own use. The Self Service Portal (SSP) provides a means for employees to use some key MDM tools without any IT involvement. If you enable it, end users can run the SSP in a web browser and access key MDM support tools. You can also enable or disable the displays of information and the ability to perform remote actions from the SSP.

End users can perform remote actions over-the-air to the selected device from within the Self Service Portal. Your administrator determines the selected device's action permissions and available actions in the SSP, which vary based on platform. Allowed actions are split between **Basic Actions** and **Advanced Actions** on the main access page.

The administrator determines action permissions, therefore device users might have limited actions available. See the applicable platform guide, available on docs.vmware.com. You can also search the online help for platform-specific options.

Basic Remote Actions in the SSP

Basic remote actions appear on the Basic Actions subtab of the selected device in the self-service portal. The actions available depend upon enrollment status, device platform, and action permissions.

Action	Description
Change Passcode	Set a new passcode for the selected device. If a device end user logs into the SSP to change a shared device passcode before it expires, this new passcode adpots the expiration time from the OG associated with the shared device, not the OG the end user is managed from. For example, assume you have an OG structure with 'Parent' at the top and 'Child' underneath. Assume that the end user account is managed from 'Parent' with a passcode expiration of 90 days. Assume also that the shared device is managed by 'Child' with a passcode expiration of 30 days. In this scenario, when the end user logs into the Self Service Portal and changes the shared device passcode before it expires, the new passcode expiration goes from 90 days (Parent) to 30 days (Child). The workaround is to ensure that you configure the shared device passcode on the OG the users are managed from. As the admin, if you change the end user's shared device passcode in the **Add/Edit User** screen from the Workspace ONE UEM console, it correctly adopts the expiration time of the OG the end user is managed from.
Clear Passcode	Clear the passcode on the selected device and prompt for a new passcode. This action is useful if users forget their device passcode and are locked out of their device.
Delete Device	Remove the device from the Self Service Portal.
Delete Registration	Delete any pending enrollment record from the Self Service Portal.

Action	Description
Device Query	Request the device to send a comprehensive set of MDM information to the Workspace ONE UEM Server.
Device Wipe	Wipe all data from the selected device, including all data, email, profiles, and MDM capabilities and returns the device to factory default settings.
Download Hub	Download and install the Workspace ONE Intelligent Hub to the device from which you are viewing the SSP.
Enterprise Wipe	Wipe all corporate data from the selected device and removes the device from Workspace ONE UEM. All the enterprise data contained on the device is removed, including MDM profiles, policies, and internal applications. The device returns to the state it was in before the installation of Workspace ONE UEM.
Locate Device	Activate the GPS feature to locate a lost or stolen device. This action is hidden when privacy settings are restrictive.
Lock Device/Screen	Locks the selected device so that an unauthorized user cannot access it, which is useful if the device is lost or stolen. End users can also use the GPS feature to locate the device.
Lock SSO	Lock the single sign-on passcode for apps on this device. The next SSO app opened will prompt for a passcode.
Make Noise	Rind a device by remotely causing it to ring.
Resend Enrollment Message	Send another copy of the initial enrollment email, SMS, or QR code to the device intended to register. As a security feature, the email address that appears in the resend enrollment message form is read-only for accounts that enrolled with a token.
Send Message	Send a message using email, phone notification or SMS to the device.
Set Roaming	Set whether roaming is enabled for this device.
Sync Device	Outfit devices with the latest company policies, content, and apps.
View Enrollment Message	See the actual email, SMS, or QR code that comprised the initial enrollment message. As a security feature, this action is not available for accounts that enrolled with a token.

Note Registration and Enrollment actions only display in the SSP when the enrollment of a selected device is still pending.

Advanced Remote Actions in the SSP

Advanced remote actions appear on the Advanced Actions subtab of the selected device in the self-service portal. The actions available depend upon enrollment status, device platform, and action permissions.

Action	Description
Generate App Token	Generate a token that the device can use to access secure applications.
Manage Email	Manage devices connected to an email account.
Review Terms of Use	Review past terms of use for this account.

Action	Description
Revoke Token	Revokes the token for a selected application.
Upload S/MIME Certificate	Upload an S/MIME Certificate for a corporate email account.

Self-Service Portal Actions Matrix

Each of the major device platforms supports various basic and advanced SSP actions in Workspace ONE UEM powered by AirWatch.

Action	Android	iOS	macOS	Win Mobile	Win 7	Win Desktop
Basic Actions						
Change Passcode.	✓					
Clear (SSO) Passcode.	✓	✓				✓
Delete Device.	✓	✓	✓	✓	✓	✓
Delete Registration.	✓	✓		✓	✓	✓
Device Query	✓	✓	✓		✓	✓
Device Wipe	✓	✓	✓	✓		
Download Hub.			✓		✓	
Enterprise Wipe	✓	✓	✓	✓	✓	✓
Locate Device.	✓	✓		✓		✓
Lock Device/Screen.	✓	✓	✓	✓	✓	
Lock SSO.		✓				
Make Noise.	✓					
Resend Enrollment Message.	✓	✓		✓	✓	✓
Send Message.	✓	✓	✓	✓	✓	✓
Set Roaming.		✓				
Sync Device.	✓	✓				
View Enrollment Message.*	✓	✓		✓	✓	✓
Advanced Actions						
Generate App Token.	✓	✓	✓	✓	✓	✓
Manage Email.				✓	✓	✓
Review Terms of Use.	✓	✓	✓	✓	✓	✓
Revoke Token.	✓	✓	✓	✓	✓	✓
Upload S/MIME Certificate.	✓	✓	✓	✓	✓	✓

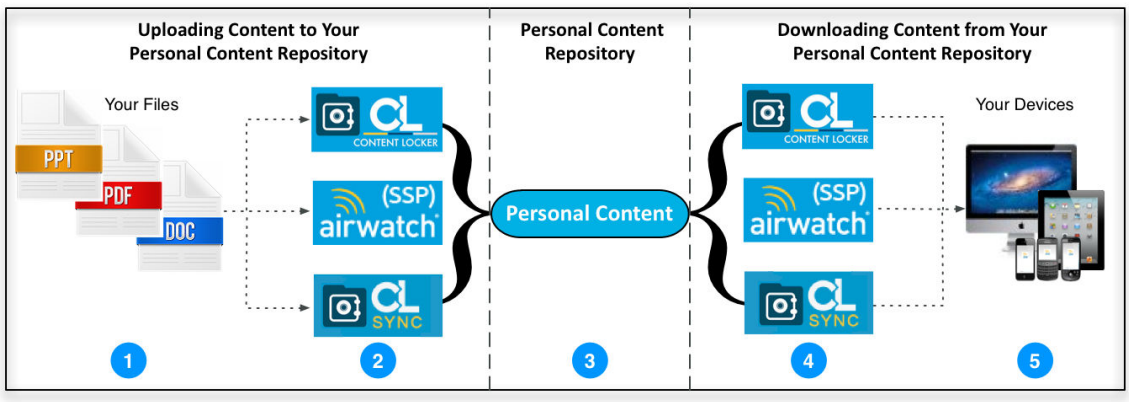
* As a security feature, this action is not available for accounts that enrolled with a token.

Personal Content, SSP

2

The Self-Service Portal (SSP) is a website unique to your organization where you can log in and see your devices managed by Workspace ONE UEM powered by AirWatch.

Personal Content refers to files you personally upload, manage, and maintain. These files are distinct from content your organization may push down to you through the VMware Workspace ONE Content app. Whereas your organization's content may be protected with the VMware Workspace ONE Content app's security functions, Personal Content is yours to control and do with as you want. You can upload and download files from your Personal Content repository in multiple ways. The diagram below illustrates these methods and the description beneath it outlines the process.



1 **Your Files** – These can be any of the supported file types that you want to access from multiple devices.

2 **Uploading Content** – You can upload Personal Content in one of three ways:

- Add content on your mobile device through the VMware Workspace ONE Content application.
- Upload content through your organization's Self-Service Portal.
- Sync content that you drop into a shared folder on your computer using VMware Content Locker Sync.

3 **Personal Content Repository** – After uploading content using one of these three methods it becomes a part of your personal content repository, which is simply a pool of all your Personal Content files.

4 **Downloading Content** – You can access this repository in one of three ways:

- Access your content from the VMware Content Locker application on your mobile device.
- View files in the Self-Service Portal by logging into your organization's website.
- Use VMware Content Locker Sync to view content from a shared folder on your laptop or computer.

5 **View Files on Devices** – The use cases for viewing personal files on devices are limitless. For example, you might drag and drop a number of important files into your VMware Content Locker Sync shared folder on your work laptop so that you can access them later on your tablet or other mobile device.

Note The availability of the VMware Workspace ONE Content app and the level of Self-Service Portal access you have is determined by your Workspace ONE UEM administrator.

This chapter includes the following topics:

VMware Content Options

Workspace ONE UEM offers three end user facing features that facilitate your organization's content management. In addition to the robust configurations and management options available within the Workspace ONE UEM console for content, you can also configure the behavior of these user facing features.

- **VMware Workspace ONE Content** – Allows end users to access important content on their devices while simultaneously safeguarding those files. Any content accessed through the VMware Workspace ONE Content opens inside the application, ensuring that it cannot be copied, saved, or shared without approval.
- **Content Locker Sync** – Allows end users to add files to a shared folder on their computers that syncs with their Personal Content repository. This folder gives them access to those files on their mobile device's VMware Workspace ONE Content app or from the Self-Service Portal.

Note Downloading, installing, and using these features are user-dependent actions. See the **VMware Mobile Content Management Documentation** for step by step instructions. See also the **Content Apps for Desktop End-User Guide** at https://resources.air-watch.com/view/jshgwzqd2fdcby73ryhf/en.These guides are available on docs.vmware.com or the my.workspaceone.com documentation repository.

For details, contact your Workspace ONE UEM Administrator.