VMware AirWatch Chrome OS Platform Guide (Legacy)

Managing Chrome OS extension with Workspace ONE UEM

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to Chrome OS Management

Chrome OS is a Linux-based operating system created and distributed by Google; it has been derived from the open-source Chromium OS. Chrome OS is designed to be used primarily while connected to the internet and most files, data, and applications are stored in the cloud.

VMware Workspace ONE UEM console™ provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Chrome OS device deployment.

Supported Devices and OS Versions for Chrome OS

Before configuring settings or prompting enrollment for Chrome OS, make sure end users are using supported devices and their OS is compatible for Chrome OS.

Supported Operating Systems

ChromeOS version 39 +

Supported Devices

Please reference the Chrome OS website for the most up to date list of supported devices.

Note: It is possible to download and use the AirWatch Agent extension on the Google Chrome Browser with Windows 7 and macOS devices. An enrollment record appears on the Workspace ONE UEM console for every browser that is enrolled.

Chapter 2:
Chrome OS Enrollment

Each Chrome OS device in your organization's deployment must be enrolled before it can communicate with AirWatch and access internal content and features. This is facilitated with the AirWatch Agent extension.

This section will cover the enrollment types you will set in the Workspace ONE UEM console and enrollment process end users are to follow to download the AirWatch Agent Extension to their Chrome OS devices.

You will have two ways for getting Chrome OS devices ready for deployment with AirWatch. You can use either of the following:

- Use your Google Admin Console to force install the Chrome OS extension to the Chrome OS devices. If this is done, end users will not be able to remove the extension from their device.
- Allow end users to install the Chrome OS extension from the Chrome Web Store. You will provide end users with a link to access the Chrome Web Store to download the extension to their Chrome OS device and then walk through the enrollment process.

Note: Please contact Google if you have any questions on how to use your Google Admin Console.

If the agent is going to be downloaded from the Chrome Web Store, admins can send a message to end users that will prompt them to enroll their Chrome OS devices into AirWatch. This message may include any of the following:

- The link the end user will use to access the Chrome Web Store to download the enrollment extension (if not being pushed with the Google Admin Console).
- A set of user credentials the end users will need to enroll their device into the Workspace ONE UEM console .
- The enrollment user token used for token enrollment, if necessary.

Email Autodiscovery

You can associate an email domain to your environment, which requires users to enter only an email address and credentials to complete enrollment.

This is a simplified approach that leverages information end users likely already know. Alternatively, if you do not set up an email domain for enrollment, users will be prompted for the Enrollment URL and Group ID, which must be given to them.

SAML Authentication

Security Assertion Markup Language (SAML) 2.0 Authentication offers single sign on support (SSO) and federated authentication. AirWatch never receives any corporate credentials because it is shared only between the user's device and their IdP.

When SAML authentication is enabled in the Workspace ONE UEM console , then after the device user enters their AirWatch Group ID, the user is redirected to the SSO user interface for authentication.

For more information on how to integrate your AirWatch environment with a SAML Provider, see the **VMware AirWatch SAML Guide**.

Enrollment Types

There are five different enrollment types available for you to configure. The enrollment type that you configure determines the steps end users need to take to establish a connection with AirWatch, and the information that you need to provide to them in the enrollment message.

Enrollment Type	Description
Basic Enrollment	Requires the Server URL, Group ID, username, and password. You will create the username and password and provide them to the user in the enrollment message.
Directory Enrollment	Requires the Server URL and Group ID, username and password. The user will already have access to their username and password which is typically assigned from their organization.
Token Enrollment	Requires a system generated token to be provided to users along with the login credentials. There are two different types of token enrollment: **Single-Factor** – Requires Server URL, Group ID, and enrollment token. **Two-Factor** – Requires Server URL, Group ID, username, password, and enrollment user token.
Autodiscovery	Requires the email address, username and password. The email address is checked to place the device in the correct AirWatch server and organization group.
SAML Authentication	Requires Server URL and Group ID. User will be redirected to their Identity Provider (IdP) server for authentication of their username and password.

Configure Enrollment Settings

Use the VMware AirWatch Agent to enroll your Chrome OS devices. The VMware AirWatch Agent provides a simplified enrollment flow for end users allowing for quick and easy enrollment.

To configure these settings:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Enrollment**.
2. Configure the following settings, as desired:

Setting	Description
Authentication Mode(s)	Enable **Basic** and **Directory** as desired. **Note:** End users utilizing SAML authentication are considered Directory users even if you select to integrate SAML without LDAP. To ensure SAML integration is successful, select the Directory checkbox under Authentication Mode(s),
Devices Enrollment Mode	Select **Registered Devices Only**.
Require Registration Token	Enable if you are going to provide users with an enrollment token.
Registration Token Types	Select the appropriate option as desired. (This option is only available if **Require Registration Token** is enabled.) • If **Single-Factor** is enabled, the end user will only have to enter the Server URL, Group ID, and enrollment token provided to enroll their devices. • If **Two-Factor** is enabled, the end user will enter the Server URL, Group ID, enrollment token, username, and password provided.

3. Select **Save**.

Create Enrollment Notification Message

You can customize messages related to Chrome OS device enrollment which provides the user information for enrolling their Chrome OS devices. This message should have all the information the user needs to enroll their device.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > General > Message Templates** and select the desired message template.
2. Configure the settings as followed:

Setting	Description
Name	Enter a subject for your enrollment message. For example, 'Chrome OS Management Enrollment'.
Description	Enter a brief description of the message intent.
Category	Select **Enrollment** from the drop-down menu.

Setting	Description
Type	Select the enrollment type from the drop-down menu. • Select **MDM Device Activation** if you will be creating new users. • Select **User Activation** if you already have users created and will be assigning the message template (which is detailed below).
Select Language	Select your desired language for the message. Select **Add** to enter additional languages.
Default	Enable the **Default** field to send the message as Email, SMS and Push Notification. If this field is disabled, configure the desired **Message Type** below.
Message Type	Select whether the message will be sent using **Email**, **SMS** or **Push** notification.

Note: If you created a message template prior to beginning set up, these fields will already be populated.

3. Edit the **Email** settings as followed:

Setting	Description
Email Content Type	Select if you email will appear in **Plain Text** or **HTML** format.
Subject	Enter a subject for your enrollment message. For example, 'Chrome OS Management Enrollment'.
Message Body	Enter the Chrome Web Store URL for the user to download the AirWatch Agent extension and the lookup values for the login credentials, for example username and password, in the **Message Body** field.

4. Select **Save**.

Add and Assign New Users the Enrollment Message Template

You can only send enrollment messages to admin added users within the AirWatch system. If you have not added any users, then you can add them to AirWatch and send them an enrollment message in the same step.

To add new users:

1. Navigate to **Accounts > Users > List View > Add > Add User** and enter the desired user information. Be sure to complete the required fields.
2. Select the enrollment message from the **Message Template** field.
3. Select **Save**.

The enrollment message is sent to end users for them to begin enrolling their Chrome OS Devices.

Assign Enrollment Message Template to Existing Users

If you already created users, you only need to send the message template to select users.

To assign the message template to existing users:

1. Navigate to **Accounts > Users > List View**.
2. Select the users from the list.
3. Click the **Send Message** button.
4. Select the enrollment **Message Template** from the drop-down menu.
5. Select **Send**.

The enrollment message is sent to end users for them to begin enrolling their Chrome OS Devices.

Enroll Chrome OS Devices

To prompt enrollment, end users will download the AirWatch Agent extension to their Chrome Web Browser and then proceed to walk through the enrollment. If you already force installed the AirWatch Agent from the Google Admin Console, the end user can proceed to enrolling the device starting at step four.

1. Select the download URL from the registration message to open the Chrome Web Store.
2. Click **Free** to begin the process.
3. Select **Add** at the confirmation screen which automatically installs the AirWatch Agent extension to the Chrome Web Browser.

   The AirWatch Agent extension icon appears at the top right of the screen with an '**AirWatch Agent has been added to Chrome**' confirmation message.
4. Click the extension and select **Enroll**:

   For **Basic** and **Directory** enrollment:

   a. Enter the **Server URL** and **Group ID** and select **Continue**.

   b. Enter the **Username** and **Password** and select **Continue**. For Directory Enrollment, the user may already know their username and password. For example, they use their username and password they use to login to their devices, so you will not create this.

   c. The next page displays a '**Your account is being managed by AirWatch**' message.

   For **Token Enrollment**:

   a. Enter the **Server URL** and **Group ID** and select **Continue**.

   b. Enter the **Enrollment User Token** and select **Continue**.

      If **Single-Factor** was selected in the system settings, you will not need to enter user credentials. Proceed to Step 7.

      If **Two-Factor** was selected, enter their **Username** and **Password** and continue to next step.

   If **Autodiscovery** was configured:

a. Select **Email** as the authentication method.

b. Enter **Email** and select **Continue**.

c. Enter **Username** and **Password**.

To use **SAML authentication** as the enrollment type:

a. Enter the **Server URL** and **Group ID** and select **Continue**.

You will be redirected to the SAML to authenticate user credentials information. If successful, you will return to the Agent to complete enrollment.

5. Select **Continue**. The next page displays a '**Your account is being managed by AirWatch**' message.

The Chrome OS is now registered with AirWatch. Select **Quit** to exit the install mode.

Chapter 3: Chrome OS Profiles

Create Chrome OS device profiles to ensure proper usage of devices, and device functionality. Profiles serve many different purposes; from letting you enforce rules and procedures to tailoring and preparing Chrome OS devices for how they will be used with AirWatch.

The individual settings you configure, such as those for restrictions and bookmarks, are referred to as payloads. In most cases, AirWatch recommends that you only configure one payload per profile, which means you will have multiple profiles for the different settings you want to push to devices. For example, you can create a profile to restrict users from saving passwords and another to block certain websites.

Device Access

Some device profiles configure the settings for accessing an Chrome OS device. Use these profiles to ensure that access to a device is limited only to authorized users.

Some examples of device access profiles include:

- Specify browser restrictions by using a Restrictions profile. For more information, see Create Chrome OS Restrictions Profile on page 10.

Device Security

Ensure that your Chrome OS devices remain secure through device profiles. These profiles configure the native Chrome OS security features or configure corporate security settings on a device through AirWatch.

- Ensure data security by forcing all personal and corporate data to be filtered through the Global HTTP proxy. For more information, see Configure Global HTTP Proxy Profile on page 11.

Device Configuration

Configure the various settings of your Chrome OS devices with the configuration profiles. These profiles configure the device settings to meet your business needs.

- Access URLs directly from the homepage. For more information, see Deploy Bookmarks Profile on page 11.

Create Chrome OS Restrictions Profile

Restrictions profiles provide a second layer of protection by allowing you to specify various browser restrictions.

To create a restrictions profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Configure the profile's **General** settings.
3. Configure **Restrictions** settings, including:

Setting	Description
Disable Autofill	Prevents any website from providing autofill suggestions when a user is filling in form data on the webpage, even if the user has previously filled in the form.
Disable Saving Password	Requires the user to enter passwords when accessing protected data and prevents the browser from automatically storing passwords.
Disable Translation Service	Turns off translation service for the browser.

4. Select **Save**.

Note: If a whitelisted website accesses resources from blacklisted website, then the website may not display properly.

Configure Website Restrictions Profile

Website restrictions allow admins to whitelist and blacklist certain websites according to the rules configured within the payload.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**
2. Configure the profile's **General** settings.
3. Select the **Website Restrictions** profiles and configure the settings, including:

Setting	Description
Allow/Block	Enter websites that to whitelist or blacklist in the provided space.
Block Images Only	Enable to allow browsing to the website but will hide the images on that page. This option only appears if **Block** is enabled.

4. Select **Save & Publish**.

Bookmarks for Chrome OS

Bookmarks provide end users with a simple way to access a URL directly from an icon located in the Chrome OS App Launcher or bookmarks bar on the Chrome Web Browser.

Bookmarks are particularly useful for easy navigation to extended URLs with a large amount of characters. End users can have bookmarks directly next to apps they use on a daily basis and connect to internal content repositories or login screens without having to open a browser to type out a long URL.

Deploy Bookmarks Profile

After setup, end user see the bookmark icon and title, selects the bookmark and connects directly to a specified URL. Admins have the ability to send bookmarks to Chrome OS devices for users to easily access.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Configure the profile's **General** settings.
3. Select the **Bookmarks** payload.
4. Configure the **Bookmarks** settings, including:

Setting	Description
Add in Chrome App Launcher	Select to add the bookmark to the app launcher. Enter the following: • Enter the bookmark Title. • Specify the link destination by entering the URL.
Add in the bookmarks Bar	Select to add the bookmark to the bookmark bar in the Chrome Web Browser. Enter the following: • Enter the bookmark **Title**. • Specify the link destination by entering the **URL**. • Provide the **Name of Parent Folder** where the bookmark is listed under in the bookmarks bar.
Add	Select add to create new bookmarks.

5. Select **Save & Publish**.

Configure Global HTTP Proxy Profile

Global HTTP Proxy settings are configured to ensure that all the HTTP network traffic is passed only through it. Using a proxy ensures data security since all the personal and corporate data is filtered through the Global HTTP proxy.

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Configure the profile's **General** settings.
3. Configure the **Global HTTP Proxy** settings, including:

Setting	Description
Proxy Type	Select the type as **Manual** or **Auto**.
Manual	Provide the complete the following fields: • **Proxy Server** – Enter the proxy server URL for HTTP, HTTPS, or FTP traffic. • **Proxy Port** – Enter the port for the corresponding proxy server. • **Exclusion List** – Add host names to prevent them from running through the proxy.
Auto	Enter the following : • **Proxy PAC File** – Paste the contents of the proxy.pac file.

4. Select **Save & Publish**.

Chapter 4: Compliance Policies

The compliance engine is an automated tool by Workspace ONE ™ UEM that ensures all devices abide by your policies. These policies can include basic security settings such as requiring a passcode and having a minimum device lock period. For certain platforms, you can also decide to set and enforce certain precautions. These precautions include setting password strength, blacklisting certain apps, and requiring device check-in intervals to ensure that devices are safe and in-contact with Workspace ONE UEM.

Once devices are determined to be out of compliance, the compliance engine warns users to address compliance errors to prevent disciplinary action on the device. For example, the compliance engine can trigger a message to notify the user that their device is out of compliance.

In addition, devices not in compliance cannot have device profiles assigned to it and cannot have apps installed on the device. If corrections are not made in the amount of time specified, the device loses access to certain content and functions that you define. The available compliance policies and actions vary by platform.

For more information about compliance policies, including which policies and actions are supported for a particular platform, refer to the **VMware AirWatch Mobile Device Management Guide**, available on docs.vmware.com.

Chapter 5:
Chrome OS Management

After your devices are enrolled and configured, manage the devices using the Workspace ONE ™ UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status. The **Device Details** page provides device-specific information such as profiles, apps, AirWatch Agent version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

Device Dashboard

As devices are enrolled, you can manage them from the Workspace ONE ™ UEM **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet and allows you to act on individual devices quickly.

You can view graphical representations of relevant device information for your fleet, such as device ownership type, compliance statistics, and platform and OS breakdowns. You can access each set of devices in the presented categories by selecting any of the available data views from the **Device Dashboard**.

From the **List View**, you can take administrative action: send messages, lock devices, delete devices, and change groups associated with the device.

Device List View

Select **Devices > List View** to see a full listing of all devices.

The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in.

Select a device in the **General Info** column at any time to open the details page for that device.

Sort by columns and configure information filters to review device activity based on specific information. For example, sort by the **Compliance Status** column to view only devices that are currently out-of-compliance and target only those devices. Search all devices for a friendly name or user name to isolate one device or user.

Customize Device List View Layout

Display the full listing of visible columns in the **Device List** view by selecting the **Layout** button and select the **Custom** option. This view enables you to display or hide Device List columns per your preferences.

There is also an option to apply your customized column view to all administrators. For instance, you can hide 'Asset Number' from the **Device List**.

Once all your customizations are complete, select the **Accept** button to save your column preferences and apply this new column view. You can return to the **Layout** button settings at any time to tweak your column display preferences.

Search in Device List View

You can search for a single device for quick access to its information and take remote action on the device.

To run a search, navigate to **Devices > List View**, select the **Search List** bar and enter a user name, device friendly name, or other device-identifying element. This action initiates a search across all devices, using your search parameter.

Device Details Page

Use the **Device Details** page to track detailed device information and quickly access user and device management actions.

You can access the **Device Details** page by either selecting a device's Friendly Name from the **Device Search** page, from one of the available Dashboards or by using any of the available search tools with the Workspace ONE UEM console .

Use the **Device Details** menu tabs to access specific device information.

Setting	Description
Summary	View general statistics such as enrollment status, compliance, last seen, platform/model/OS, organization group, contact information, serial number, power status, storage capacity, physical memory and virtual memory.
Profiles	View all MDM profiles currently installed on a device.
Apps	View all apps currently installed or pending installation on the device.
Location	View current location or location history of a device.
User	Access details about the user of a device as well as the status of the other devices enrolled to this user.

The menu tabs below are accessed by selecting **More** from the main Device Details tab.

Setting	Description
Notes	View and add notes regarding the device. For example, note the shipping status or if the device is in repair and out of commission.
Terms of Use	View a list of End User License Agreements (EULAs) which have been accepted during device enrollment.
Event Log	View history of device in relation to MDM, including instances of debug, information and server check-ins.
Status History	View history of device in relation to enrollment status.

Remote Actions

The **More drop-down** on the Device Details page enables you to perform a remove view of the selected devices. See below for detailed information about each remote action.

Note: The actions listed below vary depending on factors such as device platform, Workspace ONE UEM console settings, and enrollment status.

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Change Organization Group** – Change the device's home organization group to another pre-existing OG. Includes an option to select a static or dynamic OG.
- **Delete Device** – Delete and unenroll a device from the UEM console. This action performs an Enterprise Wipe and remove its representation in the UEM console.
- **Device Information (Query)** – Send an MDM query command to the device to return basic information on the device such as friendly name, platform, model, organization group, operating system version and ownership status.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.
- **Enterprise Wipe** – Enterprise Wipe a device to unenroll and remove all managed enterprise resources including applications and profiles. This action cannot be undone and re-enrollment will be required for Workspace ONE UEM to manage this device again. Includes options to prevent future re-enrollment and a **Note Description** field for you to add any noteworthy details about the action.
  - Enterprise Wipe is not supported for cloud domain-joined devices.
- **Profiles (Query)** – Send an MDM query command to the device to return a list of installed device profiles.
- **Query All** – Send a query command to the device to return a list of installed apps (including AirWatch Agent, where applicable), books, certificates, device information, profiles and security measures.
- **Remote Control** – Take control of a supported device remotely using this action, which launches a console application that enables you to perform support and troubleshooting on the device. This action requires Remote Control Service to be installed on the device.
- **Request Device Check-In** – Request that the selected device check itself in to the UEM console. This action updates the **Last Seen** column status.
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.