Chrome OS Platform

VMware Workspace ONE UEM 2111

vmware

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

1 Workspace ONE UEM Integration with Chrome OS 4

Setup Chrome OS Configuration Settings 5

2 Chrome OS Enrollment 6

3 How to Configure Profile for ChromeOS Devices 8

4 Chrome OS Management 23

5 VMware Workspace ONE UEM Extension for Chrome OS 26

Workspace ONE UEM Integration with Chrome OS

1

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

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

User Setup

Workspace ONE UEM needs access to the same list of users that are present in the Google Admin Console which is facilitated through Directory Integration. For more information on Directory Integration, see the Directory Services Integration Guide. For more information on how to sync users in the Google Admin Console, see the Google Cloud Directory Sync documentation from Google.

Requirements for Deploying Chrome OS

Consider the requirements from the AirWatch team before deploying Chrome OS devices. Understanding this information helps prepare you for a successful deployment of devices.

Supported Devices

Refer the Chrome OS website for the most up-to-date list of supported devices.

Chrome Enterprise Licensing

To get started with Chrome OS device management, obtain a Chrome Enterprise license for each device you want to manage. For more information about Chrome Enterprise licensing, contact your Chrome OS device reseller or your Google sales representative. You can view and manage your Chrome Enterprise licenses from the Google Admin Console. You must put in a request to use Chrome OS Management through AirWatch and obtain service account details for a successful deployment.

You must put in a request to use Chrome OS Management through AirWatch and obtain service account details for a successful deployment.

This chapter includes the following topics:

- Setup Chrome OS Configuration Settings

Setup Chrome OS Configuration Settings

The setup page from the Workspace ONE Console facilitates the integration between Workspace ONE UEM and Google for Chrome OS management. Simply enter your Google admin account and you are redirected to Google authorization page to grant permissions.

Procedure

1. Enable Chrome Device Management (CDM) API Partner Access for device and user policies under from the Google Admin Console by navigating to **Device Management > Chrome Management > Device Settings and Device Management > Chrome Management > User Settings** and select the checkbox under the Chrome Management-Partner Access section.
2. Navigate to **Devices > Device Settings > Devices & Users > Chrome OS > Chrome OS EMM Registration** in the Workspace ONE console.

   Note Make sure there is a Group ID assigned to the Organization Group or registration will fail.
3. Enter the **Google Admin Email Address**.
4. Select **Register with Google**. You are redirected to the Google login page to enter your Google admin email address.

   Ensure you have pop-ups enabled otherwise the Google authorization page will not open.
5. Select **Allow** to grant permissions.
6. Copy Google Authorization Code from Google and paste it into the **Google Authorization Code** field in the Workspace ONE console.
7. Select **Authorize**.
8. Select **Test Connection** to ensure the connection between Workspace ONE UEM and Google is established.

   If successful, a green 'Test Connection Successful' message displays.
9. Select **Device Sync** which manually syncs new Chrome OS enrollments into them Workspace ONE UEM console.

   Clear Settings appears after registration is complete. If you click this button:

   - Chrome OS device records are cleared.
   - Certificates pushed to Chrome Users or Devices from the console are revoked.
   - The Workspace ONE UEM Extension is removed from your devices. For more information on the UEM extension, see Chapter 5 VMware Workspace ONE UEM Extension for Chrome OS.

Chrome OS Enrollment

2

Each Chrome OS device in your organization's deployment must be enrolled before it can communicate with Workspace ONE UEM and access internal content and features.

Enrolled devices adhere to the Chrome management policies set in the Workspace ONE UEM console until you wipe or recover them. Enrollment occurs during the device setup of the Chrome OS device out of the box. Follow the prompts on the device until you get to the 'Sign into the Chromebook page'. A device has to be enrolled before any user signs in (including an admin). If a user signs in before enrollment, device policies do not apply, and you have to wipe the device to restart enrollment.

Device Sync and New Device Enrollment

The Workspace ONE UEM console syncs new Chrome device enrollments every 60 minutes. Syncing pulls in a list of all new Chrome OS devices enrolled since the last sync in the device list view. You can use the Device Sync option in the Chrome OS configuration to sync devices into the UEM console sooner. For more information on the Chrome OS Configuration page, see Setup Chrome OS Configuration Settings

Enroll Chrome OS Devices

Enrollment is facilitated from the Chrome OS device using the Google admin credentials or existing G Suite user credentials.

To enroll Chrome Os devices:

1 Power on the Chromebook and connect to Wi-Fi.

2 Press **CTRL+ALT+E** when prompted for a Google account to proceed to enterprise enrollment at the **'Sign into the Chromebook'** page.

3 Enter the user name and password from your Google Admin welcome letter or use your existing G Suite user credentials.

4 Enter Device information (Optional).

5 Select **Done**. Perform steps 1–5 on all devices that you want to enroll.

Note After you select done, the Chromebook automatically applies any pre-configured device policies and is ready for a user to sign in. Once a user signs in, all applicable user profiles are pushed to the Chrome device.

6 Navigate to **Devices > Device Settings > Devices & Users > Chrome OS Configuration**. Select **Device Sync** which syncs all new enrollments into the Workspace ONE UEM console.

Note If you do not select Device Sync, new enrollments are automatically synced every 60 minutes.

How to Configure Profile for ChromeOS Devices

3

Profiles serve many different purposes from letting you enforce rules and procedures to tailoring and preparing ChromeOS devices for how they are used with Workspace ONE UEM.

The individual settings you configure, such as restrictions and bookmarks, are called profiles or payloads. In most cases, consider configuring one payload per profile, which means you have multiple profiles for the different settings you want to push to devices. For example, you can create a profile to restrict users from using incognito mode.

Important When applying profiles across parent and child organization groups, the device accepts the latest profile pushed to the device not the most restrictive like other platforms. Do not apply the same payload in both a parent and child organization group to the same device.

Device Profiles

Device policies apply to ChromeOS devices regardless of any user logged into the device. Device polices are applied through Smart Groups.

Smart groups are customizable groups that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision.

User Profiles

User profiles for ChromeOS allow you to configure profile settings at the user level. The policies do not apply to users signed in as guest or with a Google Account outside of your organization (such as a personal Gmail account). You are able to view **User Details** by selecting the user icon under the **Installed Status** field.

User polices are applied through User Groups. User groups are sets of users into user groups which, like organization groups, act as filters for assigning profiles and applications.

This to Consider When Pushing Profiles

- Profiles do not have an add version option. If the profile is edited and saved, the updated policy is sent to devices.

- Profiles for ChromeOS are deployed using API calls, which are a different solution than is used with other platforms, in which the profile is sent directly to the Workspace ONE Intelligent Hub on the device. For ChromeOS devices, the UEM consolerelies on API responses to the Google Cloud to push new polices. The Console displays a green check mark to show that the policy has been updated to the Google cloud.
- Profiles do not show a 'Publish Preview'. When you select Save & Publish, the profile takes effect immediately.
- All user and device profile information, including certificates, are sent to to Google and stored by Google.
- User profiles and Device profiles are independent in their settings.

Configure Profiles

The UEM console follows the same basic steps to push all profiles. Use the section below to explore the available settings for each profile.

1 Navigate to **Resources > Profiles & Baselines > Profiles > Add > Add Profile > ChromeOS**.

2 Select **Device** to deploy settings to the device profile or **User** to deploy settings to the user profile.

3 Configure the **General** profile settings as appropriate. These General profile settings determine how the profile deploys and who receives it.

4 Select the desired profile and configure the settings as desired.

5 After you've configured all settings, select **Save & Publish**.

Network

The Network profile allows you to configure network connection settings to apply towards device policies and user policies.

Setting	
Service Set Identifier	Provide the name of the network the device connects to.
Connectivity	Indicate if the Wi-Fi network is **Hidden** or **Auto-Join**. Auto-Join indicates that the network is connected automatically when in range.

Setting	
Security Type	Specify the access protocol used and whether certificates are required. If **WPA/WPA2** is selected, the **Password** field displays. If **WPA/WPA2 Enterprise*** is selected, the following fields display: ■ **Extensible Authentication Protocol (EAP)** - Specify the EAP from the drop-down menu. ■ **Identity** - Enter a description to which is used to identify the certificate during authentication. ■ **Root Certificate** - Use the Certificates section at the bottom to add the Root Certificate. ■ **Client Certificate** - Use the Certificates section at the bottom to add the Client Certificate.
Password	Provide the password for the device to connect to the network. The password field displays when **WPA/WPA 2** is selected from the **Security Type** field.
Proxy	Enter the proxy details.
Gateway Platform	Describes the gateway address to use for the configuration. Select the gateway as **Direct Internet Connection**, **Manual Proxy Configuration**, or **Automatic Proxy Configuration** to configure settings.
HTTP Proxy Port	Enter the host name of IP address for the proxy server. This field displays if Manual Proxy Configuration is selected.
HTTP Proxy Host	Enter the target port for the proxy server. This field displays when Manual Proxy Configuration is selected.
Secure HTTP Proxy Host	Enter settings for the secure HTTP proxy. This field displays when Manual Proxy Configuration is selected.
Secure HTTP Proxy Port	Enter secure port to use for proxy. This field displays when Manual Proxy Configuration is selected.
FTP Proxy Host	Enter the host name of IP address for the FTP proxy server. This field displays when Manual Proxy Configuration is selected.
FTP Proxy Port	Enter the target port for the FTP proxy server. This field displays when Manual Proxy Configuration is selected.
SOCKS Host	Enter the settings host address for the SOCKS proxy. This field displays when Manual Proxy Configuration is selected.
SOCKS Port	Enter the target port for the SOCKS proxy server. This field displays when Manual Proxy Configuration is selected.
No Proxy for the following Domains (Comma-Separated domains)	Enter the domains whose traffic is not handled by the proxy settings. This field displays when Manual Proxy Configuration is selected.

Setting	
Autoconfiguration URL (Leave blank for WPAD protocol)	Enter the URL which defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method). This field displays when Automatic Proxy Configuration is selected.
Add Certificate*	Select whether to **Upload certificate file** or **Select certificate template**. When you select Upload Certificate, you are directed to a dialog to upload your certificated from your saved files.
Certificate Authority*	Select the Certificate Authority and the certificate template from the drop-down menu for your organization group. The certificate authorities and the templates are added for an organization group at Devices > Certificates > Certificate Authorities. This field displays if you choose **Select certificate template** from the **Add Certificate field**.
Certificate Template*	Select your certificate template and select **Add**. This field displays if you choose **Select certificate template** from the **Add Certificate** field.
File-Upload Field*	Select **Select File** to upload your saved certificate.
Password	Specify a password if the file is protected. Select **Add**. You will the certificated listed in the **Added Certificates** section.

Credentials (Device)

For greater security, you can implement digital certificates to protect corporate assets. To do this, use the Credentials profile to define a certificate authority.

Use this profile if you want to push certificates to your devices with or without a wi-fi network.

A few things will happen once you select **Save & Publish**:

- Uploaded certs will be sent to Google and distributed to devices.
- Template certificates go down to the Workspace ONE UEM ChromeOS extension. You can provision the certificate without needing to configure a wi-fi network.
- The certificate added to Credentials payload are also available in the Network profile for attaching to a wi-fi network if needed.

Sign-in Settings (Device)

The Sign-in settings profile allows you to restrict access to the device for only a set of users.

Setting	Description
Restrict Sign-In	Enable to restrict access to the device for only a set of users. When enabled, a text box displays and you can enter a comma-separated list of user names that can sign in to the device. Wildcards(*) can be used, for example, *@example.com.
Guest Mode	Enable to allow guest access to the Chrome browser. A user is not required to sign in.
Autocomplete Domain	Set the domain name used for autocomplete on the sign-in page. The user can override this domain, if needed.
SSO Idp Redirection	Enable to redirect users to a SAML SSO IDP for login to the device.
SAML SSO cookie transfer into user session	Enable to transfer SAML SSO cookies to user session. This setting allows end users to use single sign-on with their apps by simply signing into the ChromeOS device.

Security & Privacy (Device)

The Security and Privacy profile allows you to configure user data settings.

Setting	Description
Clear user data on log out	When enabled, all local user data is cleared from the device when the user logs out. Consider using this setting for shared device use cases.
Force Re-enrollment	Force re-enrollment in the event a device is reset or wiped. After a device is reset, the enrollment screen displays and the user has to re-enroll the device. Select **Do not force re-enrollment** or **Force the device to re-enroll into the previous domain**.
Device Verified Mode Required	When enabled, verified boot mode is required for device verification to succeed.

Kiosk (Device)

The Kiosk profile allows you to lock the device into a single app (kiosk) or managed guest session (shared device mode) use case until the policy is removed. If you ever switch between modes, all settings are cleared. You cannot configure and push both modes at the same time.

Use Cases

Single App mode locks the device into a single Chrome application or extension, such as Horizon for VDI-only access.

The Managed Guest Session allows anyone to access the device as a guest user. The session itself is fully customized only allowing the user to access certain websites or applications. Once the guest user session ends, all of the local data (browser history, website logins, and files) is cleared.

Managing Certificates with Kiosk Profile

It is important to note that you have to push certificates through the Workspace ONE UEM Extension, and the Extension is only configurable for a signed-in user. Therefore a user must log in to the device to retrieve the device certificate first. After that, the certificate can is accessible across the device, including within the Managed Guest Session.

The process to manage certificates on Managed Guest Sessions:

1 Admin configures a Credentials payload in the Device profile.

2 The device is enrolled.

3 User logs in which prompts the certificate to be pushed through the Workspace ONE UEM Extension and the Credentials profile.

4 User logs out.

5 Managed guest session is started and certificates, pushed in step 3, are available in the guest session for the checked out user.

Settings	Description
Kiosk Mode	Select **Single App** or **Managed Guest Session**. The available settings in the profile will change depending on which mode you select. Single App sets an app to launch automatically for single-purpose devices like a retail store kiosk. Managed Guest Session enables the Chromebook to be logged in and out as a shared user within an organization.
	Single App
Application Name	Enter **Application Name** for corresponding application ID.
Application Identifier	Enter the application identifier. Find the desired app in the Chrome Web Store and copy the ID from the URL which includes everything after the last forward slash.
Auto Login Bailout	Enable users to press the keyboard shortcut (Ctrl+Alt+S) to prevent auto start of the app at device start-up. By default, the user has 3 seconds to press a shortcut to prevent auto-launch.
Prompt for Network Offline	Enable to display network configuration prompt when the device cannot connect to the network. **Important**:If both Prompts for Network Offline and Auto Login Bailout settings are disabled, the device might become unusable when there is no Internet access and has to go through the recovery process. If the device is offline atstart-upp, the network configuration screen always displays, before auto-launch.
Extension Policy	Enable to configure applications with JSON. Refer to the app developer's documentation for the format expected by the app.
System Log Upload (Every 12 Hours)	Enable to send system logs to the Chrome Admin Console in 12-hour increments.
Device Status Alerts	Enable to receive alerts if the device is online or offline.
Send Email if Device is Offline	Enable and enter email address with comma separation if more than one. Use this setting if Monitor Online/Offline Status is enabled.

Settings	Description
Send SMS if Device is offline	Enable and enter the phone number with comma separation if more than one.
	Managed Guest Session
Managed Guest Session Name	Display name of Managed Guest Session on device sign-in screen (max 40 characters
Session Length Limit (in seconds)	Specifies the length of time in seconds after which a user is automatically logged out, terminating the session. The user is informed about the remaining time by a countdown timer shown in the system tray. Leave blank to set no limit.
	Content
Bookmark Bar	Specify whether **User can show/hide the bookmarks bar**, **Always show the bookmarks bar**, **Never show the bookmarks bar**.
Editing Bookmarks	Enable to allow users to edit bookmarks.**Note:**If this option is disabled, existing bookmarks are still available, but new bookmarks cannot be added. Users will not be able to edit or delete current bookmarks.
Managed Bookmarks	Enable to create a list of bookmarks to be pushed onto ChromeOS.
Home Button	Specify whether **User can show/hide the Home button**, **Always show the Home button**,**Never show the Home button**.
Home Page	Specify whether **Allow user to configure**, **Home page is the new Tab page**, **Set home page**.
Pop-Up Configuration	Enable to allow pop-ups and configure user settings.
URLs to Open at Startup	Enable to configure a list of websites to launch at start up. When enabled, the URL field displays to enter the URLs.
Enable URL Certificate Auto Select	Allows you to configure URLs to automatically select client certificate if the site requests a certificate. Use the **URL** field to specify websites.
	Security & Privacy
Incognito Mode	Allow users to browse the web without storing local data.
Safe Browsing	Specify whether or not Safe Browsing is turned on for users.
Users can proceed to Malicious Sites	Configure whether or not users can navigate to a potentially malicious site from a warning page.
Saving Browser History	Disables saving browser history in Google Chrome and prevents user from changing this setting. This setting also disables tab syncing which lets you access these web pages on your computer or other synced devices.
Deleting Browser History	Disables deleting browser and download history.
Remote Access Client Domain List	Configure the required domain names for remote access clients.
QUIC Protocol	Disable QUIC protocol. This is a feature enabled automatically by Google Chrome that may affect browsing data or other Security & Privacy settings. Application controls and page loads may not function as expected without disabling QUIC.

Settings	Description
	URL Access Controls
URL Allowlist	Prevents the Chrome Browser from accessing certain URLs. Select the **Add** button to add multiple URLs.
Exceptions	Specifies exceptions to the URL allowlist. Select the **Add** button to add multiple URLs.
	Application Control
Enable Application Control	Use the dropdown to select **All Chrome apps are accessible**, **Only Chrome added below are accessible**, or **Create a list of blocked Chrome apps**.
App ID	The application identifier found in the Google Play Store.
Name	The application display name.
URL Pattern	Use a custom URL for self hosted extensions. Leave blank to push from the Chrome Web store.
Pin App to Shelf (Y/N)	Enter Y to pin the app to the homescreen dock.
Allow access to credential storage	Grant this extension to access user and device certificates for authentication.
Extension Policy	Enter the JSON acquired from the extension developer.
	Hardware
External Storage Access	Configures external storage accessibility.

System Updates (Device)

The System Updates profile specifies whether Chrome device updates automatically update to new versions of Chrome as they are released.

Setting	Description
Allow Auto Update	Enable to allow device to automatically update to the latest version when available.
Allow Kiosk App to Control Target Platform Version	Enable to allow the kiosk application to set the target platform version through an extension policy.
Target Platform Version	Specify the prefix of the target version you want the device to update to if the device is on an older version. If the device is already on a version with the given prefix, then there is no effect. If the device is on a higher version, it remains on the higher version
Maximum Update Delay Duration (hours)	Specify a duration (up to 14 days) during which your devices randomly receives system updates to ensure that all devices are not using the bandwidth at a given time.

Setting	Description
Reboot After Update	Enable to require automatic reboot the device after is updated.
Release Channel	Select the type of ChromeOS build devices to receive. The default option is "The user can change the release channel". The available options in the drop down are: ■ The user can change the release channel ■ Stable channel (Fully Tested). ■ Beta channel (Upcoming changes and improvements). ■ Dev channel (Latest features, but may be unstable).

Content (User)

The Content profile allows you to push a list of bookmarks for user convenience that applies to Chrome on all platforms.

Settings	Description
Bookmark Bar	Specify whether **User can show/hide the bookmarks bar**, **Always show the bookmarks bar**, **Never show the bookmarks bar**.
Editing Bookmarks	Enable to allow users to edit bookmarks.**Note:**If this option is disabled, existing bookmarks are still available, but new bookmarks cannot be added. Users will not be able to edit or delete current bookmarks.
Managed Bookmarks	Enable to create a list of bookmarks to be pushed onto ChromeOS.
Home Button	Specify whether **User can show/hide the Home button**, **Always show the Home button**,**Never show the Home button**.
Home Page	Specify whether **Allow user to configure**, **Home page is the new Tab page**, **Set home page**.
Folder Name	Create a hierarchical folder structure of bookmarks.
URL	Enter bookmark URL.
Name	Enter name to be displayed on the UI.
Pop-Up Configuration	Enable to allow pop-ups and configure user settings.
Pop-Ups	Use the drop-down to configure if pop-ups are to be:**Allow user to control pop-up behavior**, **Allow all sites to show pop-ups**, **Do not allow any sites to show pop-ups**
Sites that can always show pop-ups	Enter URLs to be whitelisted from pop-ups.
Sites that are never allowed to show pop-ups	Enter URLs to be blacklisted from pop-ups.
URLs to Open at Startup	Enable to configure a list of websites to launch at start up. When enabled, the **URL** field displays to enter the URLs.

Settings	Description
URL Certificate Auto Select	Allows you to configure URLs to automatically select client certificate if the site requests a certificate. Use the **URL** field to specify websites.
Certificate Pattern	Select the certificate to be used when the website is accessed.

Security & Privacy (User)

The Security & Privacy profile allows you to configure incognito settings for the users.

Setting	Description
Incognito Mode	Allow users to browse the web without storing local data.
Safe Browsing	Specify whether or not Safe Browsing is turned on for users.
Users can proceed to Malicious Sites	Configure whether or not users can navigate to a potentially malicious site from a warning page.
Saving Browser History	Disables saving browser history in Google Chrome and prevents user from changing this setting. This setting also disables tab syncing which lets you access these web pages on your computer or other synced devices.
Deleting Browser History	Disables deleting browser and download history.
User Verified Mode Required	When enabled, verified boot mode is required for device verification to succeed.
Lost Mode Message	Enter a custom message that displays when a device is set to Lost Mode. Lost Mode is configured from Device Management commands in the Device Details. For more information on Lost Mode, see Chapter 4 Chrome OS Management.
Allow Android Apps to Access System Keystore	Enable to let Android apps access server or CA certificates from the system keystore for domain trust.

Time Zone (Device)

The Time Zone profile determines automatic timezone selection.

Setting	Description
Automatic Time Zone Detection	Select the type of automatic timezone detection: **Let the user decide**, **Never auto-detect time zone**, **Use IP to determine location for time zone**, **Use Wi-Fi access points to determine location for time zone**, **Use all location information to determine time zone**. If this policy is not configured, users can control automatic timezone detection using controls in Chrome settings.

URL Access Controls (User)

The URL Access controls profile allows you to blacklist certain URLs unless excepts are configured.

Setting	Description
URL Allowlist	Prevents the Chrome Browser from accessing certain URLs. Select the **Add** button to add multiple URLs.
Exceptions	Specifies exceptions to the URL allowlist. Select the **Add** button to add multiple URLs.

Application Control (User)

The Application Control profile allows you to add apps from the Google Play Store and Chrome Webstore.

Setting	Description
Chrome App Access	Use the dropdown to select **All Chrome apps are accessible**, **Only Chrome added below are accessible**, or **Create a list of blocked Chrome apps**.
Auto Install the following Chrome Apps	
App ID	The application identifier found in the Google Play Store.
Name	The application display name.
Pin App to Shelf (Y/N)	Enter Y to pin the app to the homescreen dock.
Auto Install the following Android Apps	
App ID	The application identifier found in the Chrome Web Store.
Name	The application display name.
Pin App to Shelf (Y/N)	Enter **Y** to pin the app to the homescreen dock.
Users can end processes in Task Manager	Enable to allow end user to see the end process option in ChromeOS.
Auto Install the following Chrome Extensions	
App ID	The unique identifier for the Extension can be found in Extension details or in the Chrome Web Store URL.
URL	Use a custom URL for self-hosted Extensions. Leave blank to push from the Chrome Web Store.
Name	Enter a friendly name to easily identify the Extension
Pin app to shelf	

Setting	Description
Allow access to credential storage	Grant this Extension the ability to access user and device certificates to be used for authentication.
Extension policy	Configure the Extension using the JSON format provided by the Extension developer.

Power Management (User)

The Power Management profile allows you to configure incognito settings for the users. These settings can be applies whether connected to power or running on battery:

Setting	Description
Idle time after which action is taken (in minutes)	Specify the idle time in minutes before the user's device goes to sleep or signs them out.
Action when Idle time is reached	Set whether the device goes into sleep mode, log out, shutdown, or do nothing.
Idle time after which warning is shown to user (in minutes)	Specify the length of time without user input before warning message is displayed.
Idle time after which screen is dimmed (in minutes)	Specify the length of time without user input before screen is dimmed.
Idle time after which screen is turned off (in minutes)	Specify the length of time without user input before screen is turned off.

Printing (User)

The Printing profile enables printing options in ChromeOS. You can choose either to allow using the print preview with Google cloud print or select always use system print dialog window.

Setting	Description
Printing	Enable to allow printing from ChromeOS.When disabled, printing is only possible through plug ins that bypass Google Chrome. For example, certain Flash applications that have the print option in their context menu.

Dell Device

Setting	Description
Support Assist	Dell SupportAssist is a subscription based service, which monitors device health to proactively address any potential issues, such as viruses or hardware failure. When enabled, enter the custom JSON text retrieved from Dell TechDirect in the SupportAssist Configuration field.Follow the instructions from the prerequisites section to retrieve and configure the JSON payload, see steps below in the section on SupportAssist.
Advanced Battery Charge Mode	This setting should be used in order to prolong the health of the battery during the work day. During the set schedule, AC charging will be controlled in order to keep devices at a lower, healthy charge level. Express charging will be used intermittently to maintain the percentage. Additionally, devices will only be charged to full capacity one time per day, prior to the start of the schedule. This setting will also override the Primary Battery Charge Mode during the set schedule. Outside of the schedule, devices will charge normally, or according to the Primary Battery Charge Mode.Follow the instructions in the prerequisites section to retrieve and paste the JSON text into this fieldhttps://cloud.google.com/docs/chrome-enterprise/policies/?policy=DeviceAdvancedBatteryChargeModeDayConfig
Primary Battery Charge Mode	Helps to minimize wear and extend battery life by dynamically controlling battery charging.These settings are as follows: ■ **Standard**: Battery is fully charged using the standard charge rate ■ **Express charge**: Battery is charged rapidly using fast charge technology ■ **Primarily AC use**: Extends the lifespan of the battery for devices that are usually plugged into an AC power source ■ **Adaptive**: Battery settings are dynamically optimized based on the battery usage pattern ■ **Custom**: Set custom start and stop percentage values at which the battery will begin and end charging.
Scheduled Update Configuration	Determine when and how frequently devices will wake to check and install available updates. Follow the instructions in the prerequisites section to retrieve and configure the JSON payload:https://cloud.google.com/docs/chrome-enterprise/policies/?policy=DeviceScheduledUpdateCheck

Setting	Description
Power Source Configuration	Set power source thresholds to help minimize AC consumption during peak power times of the day for countries with AC power restrictions. Use this setting to set the per-day schedule during which the Power Source Shift Threshold will be applied. The custom schedule is mandatory to enable Power Source Configuration This setting is also known as Peak Shift. Use the **Power Source Shift Threshold** to enter a battery percentage between 15-100 at which devices will shift back to AC power. Any percentage higher than the set threshold will use battery power only, even when the device is connected to an AC power source. Use **Power Source Custom Configuration** to configure JSON payload to customize AC power consumption per day. Use the guidance when configuring the JSON: ■ start_time: The time at which Power Source Shift Threshold goes into effect. This value must be less than or equal to end_time. ■ end_time: The time at which Power Source Shift Threshold stops taking effect. This value must be greater than or equal to start_time and less than or equal to charge_start_time. ■ charge_start_time: The time at which normal AC charging resumes. This value must be greater than or equal to end_time For more guidancence on the Power Source Configuration, see the Google documentation: https://cloud.google.com/docs/chrome-enterprise/policies/?policy=DevicePowerPeakShiftDayConfig
Power On When AC is Connected	Automatically wakes device from powered-off or hibernation state when AC power is connected.
Allow Power Sharing Through USB	Allows external USB devices to be charged even when devices are in sleep mode.
Device Dock MAC Address Source	This setting can be used in the case that MAC address-based network restrictions or filtering is used. You can choose the source of the MAC Address when a dock is connected. Below are the options: ■ **Use designated dock MAC address:** This is a virtual MAC address assigned to the dock ■ **Use device's built-in MAC address**: This is the physical MAC address of the ChromeOS device's built-in network card ■ **Use dock's built-in MAC address**: This is the physical MAC address of the dock's built-in network card

Configure Support Assist

The SupportAssist configuration (use to configure the Dell Settings profile) is acquired thrugh the Dell TechDirect for customers who have subscribed to the SupportAssist Service.

Dell SupportAssist is a subscription based service, which monitors device health to proactively address any potential issues, such as viruses or hardware failure. When enabled, enter the custom JSON text generated from Dell TechDirect in the SupportAssist Configuration field in the Dell profile in the UEM console.

After you've navigated to the Dell Settings profile, follow these steps to generate the SupportAssist JSON to paste in the SupportAssist field:

1 Login to Dell TechDirect.You will navigate to the SupportAssist page and accept the terms and conditions.

2 Navigate to **Assets** > **Deploy**> **Verify Account** and sign in with your MyAccount credentials that are connected to Dell TechDirect.

3 Configure SupportAssist for ChromeOS and save the settings.

4 Download the SupportAssist JSON to copy and paste into the **SupportAssist** field in the UEM console.

   The SupportAssist JSON is generated for you to copy and paste in the Workspace ONE UEM console.

Chrome OS Management

4

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, Workspace ONE Intelligent Hub 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.

Chrome OS 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.

- **Security** – View the top causes of security issues in your device fleet. Selecting any of the doughnut charts displays a filtered **Device List** view comprised of devices affected by the selected security issue. If supported by the platform, you can configure a compliance policy to act on these devices.
  - **Compromised** – The number and percentage of compromised devices (jailbroken or rooted) in your deployment.
  - **No Passcode** – The number and percentage of devices without a passcode configured for security.

- **Not Encrypted** – The number and percentage of devices that are not encrypted for security. This reported figure excludes Android SD Card encryption. Only those Android devices lacking disc encryption are reported in the donut graph.

Ownership – View the total number of devices in each ownership category. Selecting any of the bar graph segments displays a filtered **Device List** view comprised of devices affected by the selected ownership type.

- **Last Seen Overview/Breakdown** – View the number and percentage of devices that have recently communicated with the Workspace ONE UEM MDM server. For example, if several devices have not been seen in over 30 days, select the corresponding bar graph to display only those devices. You can then select all these filtered devices and send out a query command so that the devices can check in.
- **Platforms** – View the total number of devices in each device platform category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices under the selected platform.
- **Enrollment** – View the total number of devices in each enrollment category. Selecting any of the graphs displays a filtered **Device List** view comprised of devices with the selected enrollment status.
- **Operating System Breakdown** – View devices in your fleet based on operating system. There are separate charts for each supported OS. Selecting any of the graphs displays a filtered **Device List** view comprised of devices running the selected OS version.

Device Management Commands

The **More Actions** drop down on the Device Details page enables you to perform remote actions over-the-air to the selected device. The actions listed vary depending on factors such as device platform, Workspace ONE UEM console settings, and enrollment status.

- **Enterprise Wipe** Enterprise Wipe deprovisions selected Chrome OS devices from management in the Workspace ONE UEM console. Devices will continue to show as managed to the end user, but the UEM console shows the device as unenrolled in the Device Details page. All device policies are removed and policy updates are not sent to devices after the enterprise wipe. User Policies will remain intact on the device, as these are not dependent on device enrollment. In order to completely wipe device or to reenroll the device, a powerwash (full device wipe) is required.
- Before the enterprise wipe processes, choose what happens with the Chrome OS license assigned to the device. Select **Different Replacement Model**, **Retiring Device**, or **Same Model Replacement**. The reason is stored in the UEM console Event Log. For annual licences, you can simply reassign to another device. For perpetual licences:
  - Replacement devices will need to be purchased with a perpetural license upgrade.
  - The licence can be transferred to a different device with the same model.

    - If the device is being retired, any new devices purchased will need to be purchased with a Chrome Enterprise license ugprade.
- **Reboot Device** – Reboot a device remotely, reproducing the effect of powering it off and on again. Only supported on devices in Kiosk mode.
- **Device Wipe** – Allows you to wipe device which removes all apps, data, email, profiles, and MDM capabilities and resets the device to its factory state. This is a restricted action which prompts you for a pin before the action can be completed.
- **Clear User Profiles** – In the event a device is lost or stolen, this command remotely log out and delete all users on the device, including any locally saved user data. This is a restricted action which prompts you for a pin before the action can be completed.
- **Enable Lost Mode** – Allows you to remotely disable devices that have been lost or stolen. When enabled, you can set a custom message to display on the lock screen through the Chrome OS device profile. While disabled, the device cannot be used for any purpose. Devices can then be re-enabled remotely once they are found.

VMware Workspace ONE UEM Extension for Chrome OS

5

The VMware Workspace ONE UEM Extension for Chrome OS is a extension created to handle certificate management on Chrome OS devices. This extension provides direct communication with the UEM console and supports certificates for Wi-Fi, VPN, web authentication and more.

Chrome OS Extension Deployment

The deployment of the Chrome OS extension is silent for the end user, and there are no prompts that will display on the user's device. The extension is deployed automatically to known user accounts (AD sync or users added manually to the UEM console) once a user logs in. The extension directly contacts the Workspace ONE UEM console to notify of the new device enrollment. Once the UEM console syncs that device record with Google, the device and user policies will be assigned and pushed.

Thing to consider:

- The extension only functions on managed Chrome OS devices. If the device is detected as unmanaged, then the extension will not run.
- The extension is hosted on the Chrome Web Store as an unlisted application which means users will not be able to search for and download it. It can only be installed via a direct download link, which the UEM console provides in the user policy.

Certificate Types

The Workspace ONE UEM Extension offers flexible options for any use case.

- User Certificates
  - For use by only a single user.
  - Not shared with other user accounts.
- Device Certificates
  - Shared across all device users.
  - Includes login users, guest users, kiosk, and managed guest sessions.

Supported Certificate Authorities

- Microsoft ADCS
- Generic Scep

Certificate Management Through the Chrome OS Extension

A Network profile is configured under User or Device policy. The Network payload contains wi-fi information, while the Credentials payload contains certificate information. Network settings will be sent through Google cloud, while certificate details will be queued up for the extension. To get started with the Network profile, see How to Configure Profiles with Chrome OS.

The extension is notified of a new certificate policy through Firebase Cloud Messaging (FCM). The extension will retrieve certificate request instructions from the UEM console. The extension will create the CSR (certificate request) and send it to the UEM console. The UEM console then forwards the request to the certificate authority, which returns a certificate. The certificate is forwarded back down to the extension which will install the certificate onto the device.

Networks using certificate based authentication will be configured automatically. Certificates being used for other forms of authentication may need to be selected by the user during the authentication process.

Certificate details are viewable in the console under **Devices > Certificates**.

Certificates configured via User Policy are user-based and only accessible to that user. Certificates configured through Device Policy will be installed at the device level, accessible by any user or guest user/kiosk.

Device Actions

There are some device actions in the UEM console that will affects the extension. Consider the following:

- When 'Clear User Data on Logout' is enabled, the extension and any user certificates are deleted on logout.
- If you clear registration from the Chrome OS EMM Registration, the UEM Extension is removed from your devices.

Certificate Renewal and Revocation

Certificates for the Chrome OS Extension follow the renewal and revocation settings in the Certificate Authority configuration. When a certificate expires, it will be revoked by the Certificate Authority. The UEM console notifies the extension, and a new certificate is generated.

When a device is enterprise wiped or the registration is cleared, any assigned certificates are revoked.

Admins can also manually revoke and renew certificates from the UEM console.