VMware AirWatch Chrome OS Platform Guide

Managing Chrome OS Devices with AirWatch

AirWatch v9.3

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

Table of Contents

Chapter 1: Overview

Introduction to Chrome OS Management

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.

AirWatch provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Chrome OS device deployment.

Requirements for Deploying Chrome OS

Consider the following requirements from the AirWatch team before deploying Chrome OS devices. Familiarizing yourself with the information available in this section 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.

Google Admin Console Service Account

The AirWatch Console manages Chrome OS devices through integration with the Google Admin Console. AirWatch uses a service account to authenticate your organization and sandbox it from other customers managing Chrome OS devices with AirWatch. When configuring Chrome OS device management in both your AirWatch and Google Admin console, have your service account information at hand.

To obtain a service account, send an email to The AirWatch Chrome Management Team:

- Provide your Customer Name and Domain as set up in the Google Admin Console.

Your service account details are provided to you including your Client ID, Chrome Service Account Email, and Authentication Certificate. Use these details in the steps provided.

User Setup

AirWatch 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 available through AirWatch Resources.

For more information on how to sync users in the Google Admin Console, see to the Google Cloud Directory Sync documentation from Google.

Setup Google Admin Console

The Google Admin Console is where administrators manage Google services for users in an organization. AirWatch uses the Google Admin Console for integration with Android for Work and Chrome OS.

The Manage API client access page allows you to control custom internal application and third-party application access to supported Google APIs (scopes).

To set up your Google Admin Console:

1. Login to the Google Admin Console and navigate to **Security > Advanced Settings > Manage API Client Access**.

2. Fill in the following details:

Setting	Description
Client Name	Enter the Client ID obtained from AirWatch. for Chrome OS, this will be provided to you. For Android for Work, paste the ID from your service account.
One or More API Scopes	Copy and paste the following Google API scopes for either Chrome OS or Android for Work: **Chrome OS Google APIs:** Copy the APIs into the Google API scopes field on the same line separated by commas. https://www.googleapis.com/auth/chromedevicemanagementapi https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.device.chromeos **Android for Work:** https://www.googleapis.com/auth/admin.directory.user

3. (Chrome OS) Enable Chrome Device Management (CDM) API Partner Access for device and user policies under **Device Management > Chrome Management > Device Settings** and **Device Management > Chrome Management> User Settings**.

   (Android for Work) Select **Authorize**.

Setup Chrome OS Configuration Settings

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

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. Return to the AirWatch Console and navigate to **Devices > Device Settings > Devices & Users > Chrome OS > Chrome OS EMM Registration** in the Workspace ONE console.

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.

> **Caution**: Please make sure 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 AirWatch 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 the AirWatch Console.

Chapter 2:
Chrome OS Enrollment

Chrome OS Enrollment Overview

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

Enrolled devices adhere to the Chrome management policies set in the AirWatch 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 do not have to wipe the device to restart enrollment.

Device Sync and New Device Enrollment

AirWatch 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 paget to sync devices into the AirWatch Console sooner. For more information on the Chrome OS Configuration page, see Setup Chrome OS Configuration Settings on page 5

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 the Chrome OS device:

1. Power on the Chromebook and connect to Wi-Fi.
2. Press **CTRL+ALT+E** to proceed to enterprise enrollment at the 'Sign into the Chromebook' page. This function bypasses the sign-in screen.
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.
6. Navigate to **Devices** > **Device Settings** > **Devices & Users** > **Chrome OS** > **Configuration**.
7. Select **Device Sync** which syncs all new enrollments into the AirWatch Console. If you do not select Device Sync, new enrollments are automatically synced every 60 minutes.

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. For more information, see Chrome OS Profiles Overview. Once devices are enrolled, they display in the Device List View in the AirWatch Console.

Chapter 3:
Chrome OS Profiles

Chrome OS Profiles Overview

Profiles serve many different purposes from letting you enforce rules and procedures to tailoring and preparing Chrome OS devices for how they are used with AirWatch.

The individual settings you configure, such as restrictions and bookmarks, are called 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 Chrome OS 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 policies for Chrome OS 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).

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.

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 Chrome OS 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 AirWatch Agent on the device. For Chrome OS devices, the AirWatch Console relies 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.

Application Management

- Chrome apps are pushed through profiles using the Application Control profile, not through Apps & Books.

New and Updated

Configure Network Profile (Chrome OS)

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

To configure the Network profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **Device** to deploy settings to the device profile. Select **User** to deploy settings to the user profile.
3. Configure the **General** profile settings as appropriate.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Network** payload.

5. Configure **Wi-Fi** settings, including:

Setting	Description
Wi-Fi	
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.
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	
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 Host	Enter the host name of IP address for the proxy server. This field displays if Manual Proxy Configuration is selected.
HTTP Proxy Port	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.

Setting	Description
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.
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.
Certificate	
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.

6. Select **Save & Publish**.

Configure Sign-In Settings (Chrome OS)

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

To configure the sign-in settings profile:

1. Navigate to **Devices** > **Profiles & Resources** > **Profiles** > **Add** > **Add Profile** > **Chrome OS**.

2. Select **Device** to deploy to device policy profiles.

3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.

4. Select the **Sign-In Settings** profile and select **Configure**.
5. Configure the following settings as desired for your organization:

Setting	Description
Restrictions	
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.
User Experience	
Autocomplete Domain	Set the domain name used for autocomplete on the sign-in page. The user can override this domain, if needed.
Single Sign On	
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 Chrome OS device.

6. Select **Save and Publish**.

Configure Security & Privacy Profile (Chrome OS)

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

To configure security and privacy settings:

1. Navigate to **Devices** > **Profiles & Resources** > **Profiles** > **Add** > **Add Profile** > **Chrome OS**.
2. Select **Device** to deploy to device policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Security & Privacy** profile and select **Configure**.
5. Configure the following settings as desired for your organization:

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.

Configure Kiosk Profile (Chrome OS)

The Kiosk profile allows you to lock the device into a single app until the policy is removed.

To configure the Kiosk mode profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **Device** to deploy to device policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Kiosk** profile and select **Configure**.

5. Configure the following settings as desired for your organization:

Setting	Description
Kiosk	
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-hourr increments.
Monitor Online/Offline Status	Enable to receive alerts if the device is online or offline.
Device Status Alerts	
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.
Send SMS if Device is offline	Enable and enter the phone number with comma separation if more than one.

6. Select **Save and Publish**.

Configure System Updates Profile(Chrome OS)

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

To configure system updates settings:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **Device** to deploy to device policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **System Updates** profile and select **Configure**.
5. Configure the following settings as desired for your organization:

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 iss 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.
Reboot After Update	Enable to require automatic reboot the device after is updated.

6. Select **Save and Publish**.

Configure Content Profile (Chrome OS)

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

To configure content settings:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **User** to deploy to user policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Content** profile and select **Configure**.

5. Configure the following settings as desired for your organization:

Setting	Description
Managed Bookmarks	Enable to create a list of bookmarks to be pushed onto Chrome OS.
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.

6. Select **Save and Publish**.

Configure Security & Privacy Profile (Chrome OS)

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

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**
2. Select **User** to deploy to user policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Security & Privacy** profile and select **Configure**.
5. Configure the following settings as desired for your organization:

Setting	Description
Allow 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.

6. Select **Save and Publish**.

Configure URL Access Controls

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

To configure URL access controls:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **User** to deploy to user policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **URL Access Controls** profile and select **Configure**.
5. Configure the following settings as desired for your organization:

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

6. Select **Save and Publish**.

Configure Application Control Profile (Chrome OS)

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

To add apps using the application Control profile:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **User** which deploys user policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Application Control** profile and select **Configure**.

5. Configure the following settings as desired for your organization:

Setting	Description
Auto Install Android Apps using App Identifier	
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 Chrome Apps using App Identifier	
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.

6. Select **Save and Publish**.

Configure Power Management Profile (Chrome OS)

The Power Management profile allows you to configure incognito settings for the users.

To configure power management settings:

1. Navigate to **Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **User** to deploy to user policy profiles.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Power Management** profile and select **Configure**.
5. Configure the following settings as desired for your organization. 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 devicegoeso into sleep mode,log outt, 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.

6. Select **Save and Publish**.

Use Custom Settings (Chrome OS)

The **Custom Settings** payload can be used when new Chrome OS functionality releases or features that AirWatch does not currently support through its native payloads. With the **Custom Settings** payload, enter custom XML code to manually enable or disable certain settings.

To configure custom settings:

1. Navigate to**Devices > Profiles & Resources > Profiles > Add > Add Profile > Chrome OS**.
2. Select **Device** or **User**.
3. Configure the profile's **General** settings.

   These settings determine how the profile is deployed and who receives it. For more information on General settings, refer to the **VMware AirWatch Mobile Device Management Guide**, available on AirWatch Resources.
4. Select the **Custom Settings** payload and select **Configure**. Enter the custom XML in the text box. The XML code you paste will contain the complete block of code, from <characteristic> to <characteristic>.
5. Select **Save & Publish**.

Chapter 4:
Chrome OS Device Management

Chrome OS Management Overview

After your devices are enrolled and configured, manage the devices using the AirWatch 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 VMware AirWatch Dashboard. 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 AirWatch 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 AirWatch **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 choose 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 may 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 Management Commands for Chrome OS Devices

The **More 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, AirWatch Console settings, and enrollment status.

- **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 is required for VMware AirWatch to manage this device again.
- **Delete Device –** This command removes the enrolled device from the Console.

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.