macOS Device Management

Version: SaaS | Last Updated Dec 12, 2025 | 26 minute read |

Summarize |

Omnissa Workspace ONE UEM | Product Documentation | SaaS

After your devices are enrolled and configured, manage the devices using the Omnissa 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.

Device Dashboard

As devices are enrolled, you can manage them from the **Device Dashboard** in Omnissa Workspace ONE UEM.

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**.

ON THIS TOPIC

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

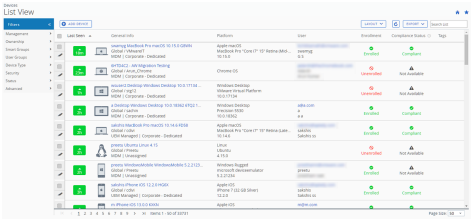
platform.

- **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.

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**.

Device List View

Use the Device List View in Omnissa Workspace ONE UEM to see a full listing of devices in the currently selected organization group.



The **Last Seen** column displays an indicator showing the number of minutes elapsed since the device has checked-in. The indicator is red or green, depending on how long the device is inactive. The default value is 480 minutes (8 hours) but you can customize this by navigating to **Groups & Settings** > **All Settings** > **Devices & Users** > **General** > **Advanced** and change the **Device Inactivity Timeout (min)** value.

Select a device-friendly name in the **General Info** column at any time to open the details page for that device. A **Friendly Name** is the

label you assign to a device to help you differentiate devices of the same make and model.

Sort by columns and configure information filters to review 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.

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.

There is also an option to apply your customized column view to all administrators at or below the current organization group (OG). For instance, you can hide 'Asset Number' from the **Device List** views of the current OG and of all the OGs underneath.

Some notable device list view custom layout columns include the following.

- SSID (Service Set Identifier or Wi-Fi network name)
- Wi-Fi MAC Address
- Wi-Fi IP Address
- Public IP Address

Exporting List View

Select the **Export** button to save an XLSX or CSV (comma-separated values) file of the entire **Device List View** that can be viewed and analyzed with MS Excel. If you have a filter applied to the **Device List View**, the exported listing reflects the filtered results.

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** > **Devices**, 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, within the current organization group and all child groups.

Device List View Action Button Cluster

With one or more devices selected in the Device List View, you can perform common actions with the action button cluster including Query, Send [Message], lock devices, and other actions accessed through the **More Actions** button.

Available Device Actions vary by platform, device manufacturer, model, enrollment status, and the specific configuration of your Workspace ONE UEM console.

Remote Assist

You can start a **Remote Assist** session on a single qualifying device allowing you to remotely view the screen and control the device. This feature is ideal for troubleshooting and performing advanced configurations on devices in your fleet.

To use this feature, you must satisfy the following requirements.

- You must own a valid license for Workspace ONE Assist.
- You must be an administrator with a role assigned that includes the appropriate Assist permissions.
- The Assist app must be installed on the device.

For more information, see the Workspace ONE Assist Guide.

Select the check box to the left of a qualifying device in the **Device List View** and the **Remote Assist** button displays. Select this button to initiate a Remote Assist session.

Device Details Page for macOS Devices

Use the Device Details page to track the 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 by using any of the available Dashboards or search tools in the UEM console.

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

Tab	Description
Summary	View general statistics on: platform/model/OS, compliance, Omnissa Workspace ONE UEM Cloud Messaging, enrollment, last seen, firewall, firmware, supervision status, time machine, contact information, groups, serial number, UDID, asset number, power status, storage capacity, physical memory and virtual memory, and warranty information. If Apple's Global Service Exchange information is accessible, select the warranty link to see when the status was last updated.
Compliance	Display the status, policy name, date of the previous and forthcoming compliance check and the actions already taken on the device. The **Compliance** tab includes advanced troubleshooting and convenience features. Non-Compliant devices, and devices in pending compliance status, have

		troubleshooting functions available. You can reevaluate compliance on a per-device basis ( ) or get detailed information about the compliance status on the device ( ). Users with Read-Only privileges can view the specific compliance policy directly from the **Compliance** tab while Administrators can make edits to the compliance policy.
	Profiles	View all the MDM profiles and their status currently installed on a device. For more information on the corrupted status of the profiles, see *Certificate Profile Resiliency*.
	Apps	View all the apps currently assigned and/or installed, including existing installed apps reported by the system. **Note:** For non-macOS devices such as Android, iOS, or Windows, the **Apps** tab displays both managed apps and all installed applications as one single list in the grid view. For macOS devices, the following tabs are displayed: **Managed Apps** - Displays all macOS application and software installers managed in Workspace ONE UEM. You can select single items in this list and perform ad-hoc Install or Remove actions. **All Apps** - Displays a list of all **.app** bundles installed on the device, reported by macOS. **Note:** By default, **Show com.apple.*apps** check box is deselected. It filters out Apple system applications to only show third-party applications.If you select **Show com.apple.*apps** check box, all installed Apple

	system apps will be displayed in the list.
Security	View the last received security information statuses from the device. Security tab shows System Integrity Protection (SIP) status, FileVault encryption status, Personal Recovery Key status, Firewall status, Supervision status, Secure Boot status (macOS 10.15 or later devices), Recovery Lock Password Status (Apple Silicon macOS 11.5 or later devices), and Managed Admin User details. For more information on accessing and rotating managed admin password, see *Admin Password Auto-Rotation*. For more information on setting and viewing recovery lock password, see *Recovery Lock Password*.
Location	View current location or location history of a device.
User	Access details about the user of a device and the status of the other devices enrolled to this user.

Additional menu tabs are available by selecting **More** from the main Device Details tab.

Tab	Description
Network	View current network status (Cellular, Wi-Fi, Bluetooth) of a device.
Restrictions	View all restrictions currently applied to a device. This tab also shows specific restrictions by Device, Apps, Ratings, and Passcode.
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.
Certificates	Identify device certificates by name and issuant. This tab also provides information about the certificate expiration.
Products	View the complete history and status of all packages provisioned to the device and any provisioning errors.
Custom Attributes	View the Custom Attributes associated with the device.
Files/Actions	View the files and other actions associated with the device.
Shared Device Log	View the history of the shared device including past check-ins and check-outs and status.
Troubleshooting	View **Event Log** and **Commands** logging information. This page features export and search functions, enabling you to perform targets searches and analysis. **Event Log** – View detailed debug information and server check-ins, including a **Filter** by **Event Group Type**, **Date Range**, **Severity**, **Module**, and **Category**. In the **Event Log** listing, the **Event Data** column can display hypertext links that open a separate screen with even more detail surrounding the specific event. This information allows you to perform advanced troubleshooting such as determining why a profile fails to install. **Commands** – View detailed listing of

	pending, queued, and completed commands sent to the device. Includes a **Filter** that allows you to filter commands by **Category**, **Status**, and specific **Command**.
Status History	View history of device in relation to the enrollment status.
Targeted Logging	View the logs for the Console, Catalog, Device Services, Device Management, and Self Service Portal. You must enable Targeted Logging in settings and a link is provided for this purpose. You must then select the **Create New Log** button and select a length of time the log is collected.
Attachments	Use this storage space on the server for screenshots, documents, and links for troubleshooting and other purposes without taking up space on the device itself.
Terms of Use	View a list of End User License Agreements (EULAs) which have been accepted during the device enrollment.

Certificate Profile Resiliency

Workspace ONE repushes profiles containing credential payloads when the certificate is detected as missing in the device Certificate List sample.

When a profile with a certificate payload is installed on a device and if the certificate goes missing from the keychain on the device, Workspace ONE reissue the certificate to the device. Certificates can go missing due to a number of reasons, but most commonly due to the following:

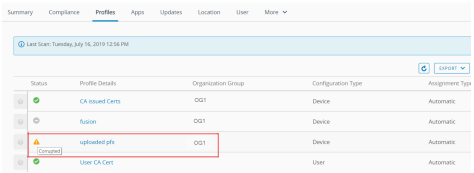
- The certificate does not install properly

in the keychain.
- Some installed software (such as security tools) on the device removes the installed certificate.
- The end-user manually removes the certificate from the keychain.

Note: The certificate will only be repushed to the device if the system detects that it is missing from the Certificate List sample. No certificates will be pushed after the initial profile installation if the sample confirms that it is installed. To prevent looping, the reinstall command is queued only one time until a successful response is received from the device.

Corrupted State Detection

Each time the system receives a certificate list sample from the device, a check is conducted to determine if there are any missing certificates based on the device's assigned profiles. If a certificate is detected as missing, the profile certificate is considered to be in **Corrupted** state and the device profile status is set to **Not Installed**.



In this scenario, when a device profile status is set to **Not Installed**, a command is queued automatically to reinstall the profile on the device. Reinstalling the profile reinstalls the certificate to the device. The following certificate types are not supported:

- User Certificate (S/MIME)
- SCEP

Admin Password Auto-Rotation

From the UEM console, you can view the password of the macOS device admin account that is created during the DEP enrollment. To help re-secure the admin accounts, these passwords are automatically rotated 8 hours after they are accessed.

Prerequisites

Device must be DEP enrolled with a DEP profile with the **Unique Random Password** enabled for the admin account.

To view the password in Device Details:

1. Navigate to **Devices** > **Devices** and select a macOS device.
2. Select the **Security** tab and then select **View Admin Password** under the **Managed Admin User** section. The **View Admin Password** page appears displaying the current password with the timestamp it was set. You can also view the password using the following API:

Explain this code

```
GET
/api/mdm/devices/<DeviceUUID>
admin-information
```

What to do next:

When the admin password is viewed from the Device Details page on the UEM console or accessed using an API, an MDM command is automatically queued to rotate the admin password after 8 hours. The event logs show logs for when the password was accessed and when it was rotated in the **Troubleshooting** section.

Note: Alternatively, the following API can also be used to rotate passwords on-demand:

Explain this code

```
POST
/api/mdm/devices/<DeviceID>/comma
command=RotateDEPAdminPassword
```

Lock Devices

From the **Device Details** page, you can lock the devices. To lock a device, perform the following steps:

1. From the device list view, Click **Lock**.
2. Enter a six digit unlock PIN for your device.
3. Enter the message that needs to be displayed on the device's PIN lock screen.

4. Click **Lock Device**.

You can view the device status message using **Security** tab. To view the device status:

1. From the device list view, click **Security** > **MDM**.
2. Click **View Device Lock Pin** to check the PIN and the last reported date.

Note: If the device is unlocked, you can view the message that the device is unlocked. When the device lock pin is accessed, it is reported in the event log. You can view the event log by navigating to **List View** > **Troubleshooting** > **Event Log**.

Recovery Lock Password

You can set the recovery lock password for an enrolled Apple Silicon macOS 11.5 and later devices through MDM Commands V3 Admin API.

The following APIs are used to issue the `SetRecoveryLock` command:

- `POST /api/mdm/devices/<DeviceUUID>/commands/SetRecoveryLock`
- `POST /api/mdm/devices/commands/SetRecoveryLock/device/<searchBy>/<AlternateID>`

Ensure that V3 admin API must be included in the header and `clear_password` is set to false in the API request.

For example, When making an API call, include below header:

```
Accept : application/json; version=3
```

Additional details must be inlcuded in the body of the API call. For example:

Explain this code

```
{
    "set_recovery_lock": {
    "current_password": "",
    "clear_password": false,
    " password_policy":

{ "length": 10,
"include_numbers": true,
"include_letters": true,
"include_special_characters":
true }
}
```

Field	Data Type	Description
Current_password	String	Optional. The c password set or provided,used f command to se clear the existir provided, the la through Worksp be used.
Clear_password	Boolean	Optional. If set password policy clears the passv device. Also dis password
Password_policy	-	Optional. Speci the Recovery Lo generated and part of the Set command. If all include_num include_let include_spe are false, then t contain all the c

The following GET Security info API return the new key `IsRecoveryLockEnabled` for macOS device:

- `GET /api/mdm/devices/<Device ID>/security` – Retrieves the security information of the device identified by the device ID.
- `GET /api/mam/devices/security/<searchBy>/<AlternateID>` – Retrieves the security information of the device identified by the alternate ID of the device.

The following GET API retrieves the device Recovery Lock Password information for a macOS device identified by the device UUID:

```
GET
/api/mdm/devices/<DeviceUUID>/sec
urity/recovery-lock-password
```

In the UEM Console, you can also view if the recovery lock is set or not in the device details page.

To view the Recovery Lock status in Device Details:

1. Navigate to **Devices** > **Devices** and select a macOS device.
2. Select the **Security** tab and then navigate to **Recovery Lock Password** section.

   The password status is displayed if it is set or not.

3. To view the password, click **View Recovery Lock Password**.

   The recovery key displays the applied password with the timestamp. It also displays the submitted password that is still not accepted by the device.

View the Recovery Lock Event Log

When the `SetRecoveryLock` command is requested, confirmed, or when the recovery password lock is accessed in the device details page or via the API, it can be viewed in the UEM console. These events are tracked in **Troubleshooting** tab in the Device Details page. To view them:

1. Navigate to **Devices** > **Devices** and select a macOS device.
2. Navigate to **Troubleshooting** > **Event Log**.

Erase All Contents and Settings (EACS)

EACS allows the administrators to make a used macOS device ready for another user, with a simple, clean workflow. It wipes all the personal content from the device and reverts the settings to the default state without the

need to reinstall the OS. When the process is complete, the device is ready to be set up from scratch.

Note: EACS option is available only for macOS 12.0.1 with Apple Silicon or the Apple T2 Security chip, and later devices. If you want to perform device wipe on older versions of macOS devices, you can send an MDM command to wipe a device clear of all data and operating system.

The following API is used to perform a EACS action on a macOS device. You can search by MacAddress, Udid, SerialNumber, ImeiNumber, or EasId.

- `POST : /api/mdm/devices/commands/DeviceWipe/device/{searchBy}/{id}`
- `POST : /api/mdm/devices/{deviceUuid}/commands/DeviceWipe`

To perform a device wipe action:

1. Navigate to **Devices** > **Devices** > Select the macOS device.
2. Navigate to **More Actions** > **Device Wipe**.
3. In the **Restricted Action - Device Wipe** page, select the **Obliteration Behaviour**. Choose from the following options:

Settings	Description
Default	The device responds to the server with an error status or no status, and then attempts obliteration.
Do Not Obliterate	The device responds with an error status, and no obliteration occurs.
Obliterate With Warning	The device responds with an acknowledgement or warning status, and then attempts obliteration.

Note: This option is available for oly macOS 12.0.1 and later devices.

4. Click **Continue**.
5. In the **Confirm Security PIN** page, enter the **Unlock Pin** and the PIN.

   A message is displayed that the device wipe command is successfully requested on the device.

Device Actions

Perform common device actions with the action button cluster including Query, Send, and other actions accessed through the **More Actions** button.

Device Details Action Button Cluster

Note: Available Device Actions vary by device model, enrollment status and type, and the specific configuration of your Workspace ONE UEM console. For more information on full listing of remote actions that you can invoke using the UEM console, refer **Workspace ONE UEM Mobile Device Management Guide**.

Run commands remotely to individual (or bulk) devices in your fleet. Each of the following device actions and definitions represents remote commands that you can invoke from the UEM console.

- **Add Tag** – Assign a customizable tag to a device, which can be used to identify a special device in your fleet.
- **Apps (Query)** – Send an MDM query command to the device to return a list of installed apps.
- **Certificates (Query)** – Send an MDM query command to the device to return a list of installed certificates.
- **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.

- **Change Ownership** – Change the Ownership setting for a device, where applicable. Choices include Corporate-Dedicated, Corporate-Shared, Employee Owned and Undefined.
- **Delete Device** – Delete and unenroll a device from the console. Sends the enterprise wipe command to the device that gets wiped on the next check-in and marks the device as **Delete In Progress** on the console. If the wipe protection is turned off on the device, the issued command immediately performs an enterprise wipe and removes the device representation in the 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.
- **DeviceWipe** - Send an MDM command to wipe a device clear of all data and operating system. This puts the device in a state where recovery partition will be needed to reinstall the OS. This action cannot be undone.
- **Edit Device** – Edit device information such as **Friendly Name**, **Asset Number**, **Device Ownership**, **Device Group** and **Device Category**.
- **Enroll** – Send a message to the device user to enroll their device. You may optionally use a message template that may include enrollment information such as step-by-step instructions and helpful links. This action is only available on unenrolled devices.
- **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.

- **Location** – Reveal a device's location by showing it on a map using its GPS capability enabled via the macOS Workspace ONE Intelligent Hub. Also requires user approval to enable the functionality in macOS System Preferences.
- **Lock Device** – Send an MDM command to lock a selected device, rendering it unusable until it is unlocked.
- **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 Workspace ONE Intelligent Hub, where applicable), books, certificates, device information, profiles and security measures.
- **Reboot Device** – Send an MDM command to restart macOS 10.13+ devices remotely. This action reproduces the effect of powering the device off and on again.
- **Security (Query)** – Send an MDM query command to the device to return the list of active security measures (device manager, encryption, passcode, certificates, etc.).
- **Send Message** – Send a message to the user of the selected device. Choose between **Email**, **Push Notification** (through AirWatch Cloud Messaging), and **SMS**.

- **Start AirPlay** – Stream audiovisual content from the device to an AirPlay mirror destination. The MAC address (format “xx:xx:xx:xx:xx:xx” with no case-sensitive) of the destination is required. A passcode can also be specified if required. Scan Time defines the number of seconds (10-300) to spend searching for the destination. Requires macOS 10.10 or greater.
- **Install macOS Workspace ONE Intelligent Hub** – Send an MDM command to the device to install the latest seeded macOS Workspace ONE Intelligent Hub.
- **Managed settings** – Managed settings lets you enable or Bluetooth through an MDM command. Requires macOS 10.13.4 or greater.
- **Shut Down** – Send an MDM command to shut down macOS 10.13+ devices remotely.
- **Request Device Log** - You can retrieve detailed logs related to operations taken by Workspace ONE Intelligent Hub from corporate-owned macOS devices and access them in the console to quickly resolve issues on the devices.

  The Request Device Log option in the UI is available only for enrolled macOS devices with Hub version 20.05 and above installed.

  For more information, see *Request Device Logs*.

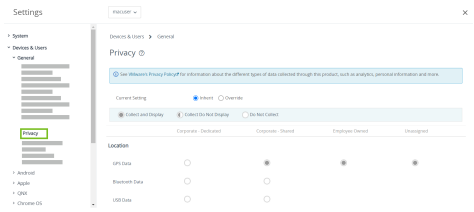
Request Device Logs

You can access the logs from the console to review both Hub and relevant system logs to aid in troubleshooting issues on the device. The Request Device Log dialog box allows you to customize your logging request for macOS devices with Hub 20.05+ installed.

Request Device Logs from the Console

Prerequisites

- Intelligent Hub 20.05 installed.
- Navigate to **Groups & Settings** > **All Settings** > **Devices and Users** > **General** > **Privacy**.



In **Current Setting**, you have the following menu items:

Explain this code

```
-   Collect and Display.
-   Collect Do Not Display.
-   Do Not Collect.
```

- Scroll down to **Request Device Log**. By default, **Collect and Display** is selected.

Note: Employee-owned devices are not allowed to be selected due to privacy concerns.

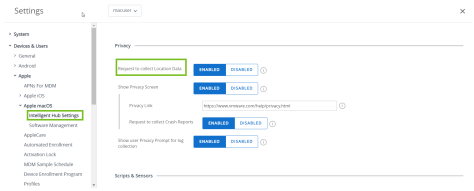
1. Navigate to **Devices** > **Devices**.
2. Select a macOS device from the list and then navigate to **More Actions** > **Request Device Log**.
3. In the **Request Intelligent Hub Logs** page, customize the log settings.

Setting	Description
Type	Determine the type of the logs to be included. (**Snapshot** or **Timed**). **Snapshot** - Select **Snapshot** to retrieve the latest log records available from devices immediately. Multiple log files will be sent to Workspace ONE UEM in the form of a ZIP file. **Note:** If you have selected **Snapshot**, the option **Level** is not available. By default, the **Level** is set to **Info**. **Timed** - Select **Timed** to collect a rolling log over a specified period. Multiple log files will be sent to Workspace ONE UEM in

	the form of a ZIP file. The option **Level (Info** or **Debug)** is available. Select the **Duration** for the log collection from the drop-down menu.
Level	Determine the level of details to be included in the log **Info** or **Debug**. **Info** - Select **Info** to collect the logs in their default state. **Debug** - Select **Debug** to enable additional advanced verbose logging. If you want to stop the debug logging before the Timer is over, and request the logs immediately, navigate to **Device Details View** > **More Actions** > **Stop Debug Logging**
Request User Consent	Select **Enabled** to request user consent for collecting logs and system files. The privacy prompt contains the information about the data collected in the logs and it requires the user acceptance before the logs are transmitted. To know more about the data collected during the log collection such as device info, crash details, install logs, see *Workspace ONE UEM Device-Side Logging* in **Workspace ONE UEM Troubleshooting and Logging** guide.

4. Select **Save**.
5. To review the log files, navigate to **Device Details** > **More** > **Attachments** > **Documents**.

To require the user consent whenever the user sends logs, navigate to **Settings** > **Device and Users**> **Apple macOS** > **Intelligent Hub and Settings**> **Show user Privacy Prompt for log collection** and **Enabled** and Save the settings.



- To retrieve the detailed logs from corporate-owned macOS devices and view them in the console, navigate to **Intelligent Hub**> **Help** and click **Collect and Send Logs**.
- To request the debug log on the device, click **Debug Session** > **Start Session**.

  Note: It collects the debug logs for specific amount of time and displays the time remaining.

- If you want to end the session, select **End Session**.

  Note: If you select **Show in Finder**, it allows you to see the logs locally in a ZIP file that can be used to troubleshoot. If you select **Send**, it allows you to send the logs to console.

Configure and Deploy a Custom Command to a Managed Device

Omnissa Workspace ONE UEM enables administrators to deploy a custom XML command to managed Apple devices. Custom commands allow more granular control over your devices.

Use custom commands to support device actions that the UEM console does not currently support. Do not use custom commands to send commands that exist in the UEM console as Device Actions. Samples of XML code you can deploy as custom commands are available at https://github.com/euc-oss/euc-samples/tree/main/UEM-Samples.

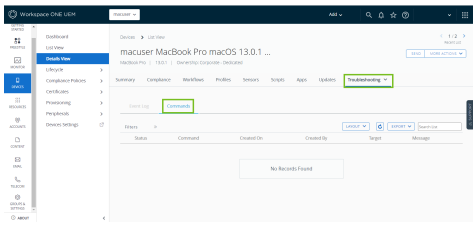
Important: Improperly formed or unsupported commands can impact the usability and performance of managed devices. Test the command on a single device before issuing custom commands in bulk.

1. In the UEM console, navigate to **Devices** > **Devices**.

2. Select one or more macOS devices using the check boxes in the left column.
3. Select the **More Actions** drop-down and select **Custom Commands**. The Custom Commands dialogue box opens.
4. Enter the XML code for the action you want to deploy and select **Send** to deploy the command to devices.

Browse XML code for Custom Commands at https://github.com/euc-oss/euc-samples/tree/main/UEM-Samples.

If the Custom Command does not run successfully, delete the command by navigating to **Devices** > **Devices**. Select the device to which you assigned the custom command. In the Device **Details View**, select **More** > **Troubleshooting** > **Commands**. Select the Command you want to remove, and then select **Delete**. The Delete option is only available for Custom Commands with a Pending status.



AppleCare GSX

Apple Global Service Exchange (GSX) allows administrators to look up device details related to the display model name, the device purchase and warranty status directly from the UEM console.

If any devices in an organization group are missing a display model name, then a time scheduler runs periodically to search and update these names using the GSX information that was configured for the devices at that organization group level.

Only authorized Apple employees or organizations that have registered with Apple's Self-Servicing Account Program can access GSX information.

Create a GSX Account

Before you can integrate your deployment, you must create an Apple GSX account. To apply for a GSX account, you must have a service contract with Apple. Contact your Apple Account Executive to learn more about GSX.

To apply for a GSX account, visit http://www.apple.com/support/programs/ssa/.

Obtain an Apple Certificate to Integrate AppleCare GSX

To integrate AppleCare GSX with your Workspace ONE UEM deployment, you must first obtain an Apple certificates and convert them to .p12 format.

For more information, see *Obtain an Apple Certificate to Integrate AppleCare GSX*.

Configure AppleCare in the UEM console

Once you have obtained and configured an Apple Certificate, you must upload the certificate to the UEM console and configure your AppleCare instance.

For more information, see *Configure AppleCare GSX in the UEM console*.

Obtain an Apple Certificate to Integrate AppleCare GSX

To integrate AppleCare GSX with your Workspace ONE UEM deployment, you must first obtain an Apple certificate and convert them to .p12 format.

1. Generate a certificate signing request (CSR) using OpenSSL or Java Keytool.
2. Send the CSR and the following GSX account information to Apple to receive Apple certificates (.pem files).

    a. GSX Sold-To account number

    b. Primary IT contact name

    c. Primary IT contact email

    d. Primary IT contact phone number

e. Outgoing static IP address of the server that sends requests to GSX Production

If your environment is hosted on the AW SaaS, refer to https://kb.omnissa.com/s/article/2960995 for the IP address. If the IP range for your environment is not listed, please open a support ticket to have our Network Operations team facilitate it.

Apple generates the Apple certificate(.pem) and returns a signed certificate and a chain certificate. For ease of use, rename the files “cert.pem” and “chain.pem” for use in subsequent steps.

You may also receive a file labeled “issuer” that is not needed for this process.

3. Convert the Apple certificates to .p12 format.

   a. Create a .p12 file using the private key and Apple certificates by executing the following command: `sudo openssl pkcs12 -export -inkey privatekey.pem -in cert.pem -certfile chain.pem -out GSX_Cert.p12`

   b. The certificate saves as a .p12 file in the location you specified. If you do not specify a path before the file name when running the conversion command, the file saves to your working directory.

Configure AppleCare GSX in the UEM Console

Once you have obtained and configured an Apple Certificate, you must upload the certificate to the UEM console and configure your AppleCare instance.

1. Navigate to **Groups & Settings** > **All Settings** > **Devices & Users** > **Apple** > **AppleCare**.

To configure a GSX connection with the UEM console, you must have a GSX account with manager-level access, access to web services, and access to coverage and warranty information.

2. Enter **GSX settings** including:

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

4. Select **Save** to complete the integration with AppleCare.
5. Navigate to the **List View**, select a device, and use the **More** menu to find **AppleCare** information in the UEM console.

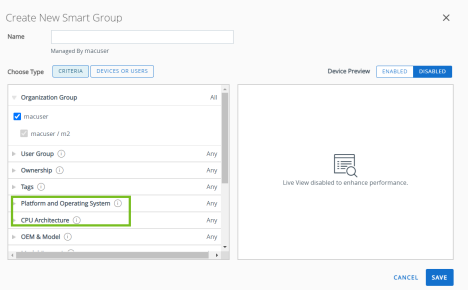
Support of Apple Silicon Mac Processor

With the introduction of Apple Silicon Macs, administrators may need to separate assignments based on CPU type. Workspace ONE UEM now provides the administrator the ability to select the processor type for an enrolled macOS device in **Smart Groups**, filter the devices based on the processor type in **Device List View**, and view the processor type info in the **Device Details** page.

Create a Smart Group

You can select the processor type while creating a Smart Group.

1. Navigate to **Groups & Settings** > **Assignment Groups** > **Add a Smart Group**.



2. In **Platform and Operating System**, select **Apple macOS**.
3. In **CPU Architecture**, select from the options:
    - Any
    - Apple Silicon (ARM64)
    - Intel (X86)
4. Click **Save**.

View the Processor Type

Device Details page allows you to view the devices based on the processor type.

1. Navigate to **Devices** > **Devices**.
2. **CPU Architecture** will be listed in the **Device Info** section

Note: When an older version of Workspace ONE Console is upgraded to the version in which this feature is supported (2107), there would be a slight delay in detecting the processor architecture information of a device. This is because the devices have to send the DeviceInformation sample after the upgrade and it happens during the next sample schedule. The CPU Architecture information would be shown as Unknown before the update and the Workspace ONE Console triggers Smart Group reconciliation once the sample data has been received.

Filter Devices Based on the Processor Type

You can now filter devices based on the processor type.

1. Navigate to **Devices** > **Devices**
2. On the left side filter, select **Device Type** > **CPU Architecture**.
3. Select the desired types and **Apply** the filter.

Managed Device Attestation

Managed Device attestation protects your device from threats. Omnissa Workspace ONE UEM accomplishes this by querying devices for their attestation certificates. The MDM server evaluates the attestation, marking the device as “Compromised” if any discrepancies arise between the attestation certificate attributes and the device attributes.

Workspace ONE UEM supports Managed Device attestation through:

- **Attestation Certificates** - These verify the authenticity of device attributes, including serial number, UDID, and OS version.

For more information about Managed Device Attestation, see Managed Device Attestation for Apple devices.

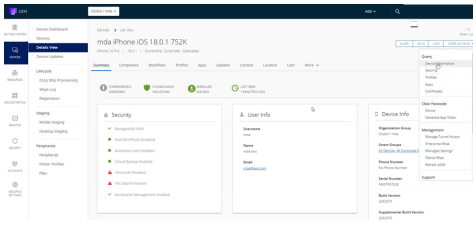
Supported Devices

Managed Device Attestation is available for iOS 16, iPadOS 16.1, macOS 14 or tvOS 16, or later.

Procedure

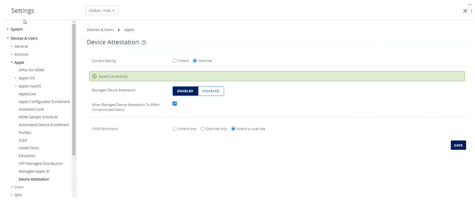
1. In the UEM console, navigate to **Devices** > **Details** > **List View**.
2. Select a device, then click **More Actions** > **Query** > **Device Information**.

The displayed data updates every 4 hours as part of the query. However, the managed device attestation query runs every 15 days.

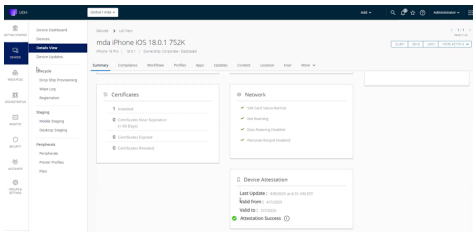


The Device Summary page shows that the device status is **Compromised Unknown**.

3. Navigate to **Settings** > **Device and Users** > **Apple** > **Device Attestation** and select **Enable**.



4. Query the device again. Check the **Events** to view the logs indicating that the Apple Managed Device attestation was sent to the device.
5. To verify successful device attestation, go to **Devices** > **Details** > **Summary**.



On the Device Summary page, you can confirm that Device is not compromised and the Device attestation is successful. You will also see the last update time, the certificate received from the device, and its validity.