

## Instructions for Removing Security Features (Remote Locks, Account Locks, Activation Locks)

### iOS

#### Apple ID / "Find My" (FMI)

##### iPhone & iPad

Official Link: [How to factory reset your iPhone, iPad, or iPod touch - Apple Support](#)

##### Procedure:

1. Open **Settings** > **General** > **Transfer or Reset [Device]**
2. Tap **"Erase All Content and Settings"**
3. Enter the device passcode or Apple ID if prompted
4. Wait until the erase process is completed

##### MacBook & iMac & Mac mini & Mac Studio

Official Link: [Erase your Mac and reset it to factory settings - Apple Support](#)

##### Procedure:

1. On the Mac, go to: **Apple Menu** > **System Settings** > **General** > **Erase All Content and Settings**
2. Follow the on-screen assistant and enter the user password if required
3. All data, user accounts, and Apple services will be removed
4. Ensure that **Find My Mac / Activation Lock** is deactivated

### Apple Watch

Official Link: [Unpair and erase your Apple Watch - Apple Support](#)

##### Procedure:

1. **Remove Apple Pay cards (if applicable):**
  - Open the **Wallet app** on the Watch
  - Tap on the card
  - Select **"Remove"**
2. **Unpair using iPhone (recommended):**
  - Keep the Apple Watch close to your iPhone
  - Open the **Apple Watch app** on the iPhone
  - Go to: **My Watch** > **All Watches**
  - Tap the "i" next to the watch
  - Select **Unpair Apple Watch**
  - Enter your Apple ID to disable Activation Lock
  - Confirm with **"Unpair"**

3. **If the watch is no longer paired (manual reset):**
  - On the Watch: **Settings > General > Reset > Erase All Content and Settings**
  - Enter the passcode if prompted
  - Confirm with **“Erase All”**
  
4. **Check and remove Activation Lock via iCloud (Optional but recommended):**
  - Go to: <https://www.icloud.com>
  - Sign in with your Apple ID
  - Click **Find iPhone > All Devices**
  - Select the Apple Watch
  - Click **Erase Apple Watch**
  - Then click **Remove from Account**

**Apple Business Manager (ABM), Apple School Manager (ASM) / Apple DEP**

Official Link: [Release devices in Apple Business Manager – Apple Support \(UK\)](#)

Official Link: [Delete a third-party MDM server in Apple Business Manager – Apple Support \(UK\)](#)

**Procedure:**

**Step 1:** Log in to ABM / ASM

1. Open the relevant website:
  - [Apple Business Manager](#)
  - [Apple School Manager](#)
2. Sign in with your administrator account.

**Step 2:** Search & select device(s)

1. Go to **Devices** in the left menu.
2. Enter the device's serial number or IMEI in the search field.
3. Select the device(s) by ticking the checkbox.

**Step 3:** Remove device(s) from organisation

1. Klick **Remove Devices** (or **Release Devices**) at the top right.
2. Confirm your selection in the dialog box.

**Step 4:** Check & revoke MDM assignment

1. If the device is still assigned to an MDM server:
2. Select the device → choose **Remove MDM Server**.

**Step 5:** Reset the device

- Perform a factory reset on the device:
  - ➔ Settings → General → Reset → Erase All Content and Settings  
(or alternatively via DFU mode)
- After the reset, no DEP-related activation lock will remain active.

**Important notes:**

- DEP (Device Enrollment Program) is now part of ABM/ASM.
- Removing devices from ABM/ASM automatically lifts automatic MDM assignment.
- The device may still need to be deleted separately in the MDM console to fully end management.
- Removal can take up to 24 hours. After that, the device is no longer bound to an MDM and can be re-enrolled by another organisation.

## Android

### Google ID / Manufacturer Account / Google Factory Reset Protection (FRP)

Official Link: [Perform a factory reset on your Galaxy phone or tablet](#)

Official Link: [How to factory reset your Google Pixel phone - Pixel Phone Help](#)

**Procedure** (may vary slightly by device):

1. Open the **Settings app**
2. Go to: **Settings > Accounts > Google > Remove account**
3. Then: **Settings > Accounts > Manufacturer Account > Remove account**
4. Then: **Settings > Accounts > Microsoft (if present) > Remove account**
5. Navigate to: **System > Reset options > Erase all data (factory reset)**
6. Confirm with your device PIN or Google account if prompted

#### Note on Google FRP

To prevent the device from remaining locked after the reset, **the Google account and any manufacturer account must be removed before performing the factory reset.**

#### Important:

If these accounts are not removed beforehand, the new user will be required to log in with the original Google credentials after the reset!

### Samsung Knox Mobile Enrollment (KME)

#### Procedure:

**Step 1:** Log in to Samsung Knox

1. Open the website: [central.samsungknox.com/login-navigator](https://central.samsungknox.com/login-navigator)
2. Sign in with your **admin account**.

**Step 2:** Find device(s)

1. In the main menu, go to **Devices**.
2. Search for the device by **serial number** or **IMEI**.
3. Select the device(s) by checking the box.

**Step 3:** Remove device(s) from Knox

1. Click **Remove Devices** in the top menu.
2. Confirm your selection in the dialog window.

**Step 4:** Check assignment to profiles (optional)

1. If the device is still assigned to a **KME profile**:
2. Remove it under:  
**Profile Management** → **Device List** → **Remove Device**

**Step 5:** Reset the device

- Perform a **factory reset**:

→ Settings → General Management → Reset → Factory Data Reset  
(or via Recovery/Download Mode)

- After the reset, **no MDM profile will be loaded.**

**Important notes:**

- Devices enrolled via **Knox** are protected by forced MDM on reset.
- Removing from **KME** lifts this binding.
- Also verify the device is removed from the MDM console (e.g., Intune, SOTI, MobileIron).
- The device is removed from KME.
- On the next reset, **automatic MDM enrollment will no longer be forced.**
- The removal is **permanent** unless the device is re-enrolled via Knox.

## **Android Zero-Touch / Android Enterprise**

Official Link: [Zero-touch enrollment for IT admins - Android Enterprise Help](#)

**Procedure:**

**Step 1:** Sign in to the Zero-Touch Portal

1. Open the website:  
<https://partner.android.com/zerotouch>
2. Sign in with your **Zero-Touch Google account** (Gmail or business Google account).

**Step 2:** Find device(s)

1. Click **Devices** in the left-hand menu.
2. Use the search field to search by **IMEI, serial number** or **username**.
3. Select the desired device(s) using the checkbox.

**Step 3:** Remove device(s) from Zero-Touch

1. Click **Remove** at the top..
2. Confirm the selection in the confirmation dialog.

**Important:**

- After removal, the device **will no longer receive automatic MDM assignment** on the next factory reset.
- The device **can be re-registered by other organisations.**

**Step 4:** Check assignment to configuration profile (optional)

1. If the device is still assigned to a configuration profile:
2. Go to:  
**Configurations** → **Select profile** → **Edit devices** → **Remove device**

**Step 5:** Reset the device

- Perform a **factory reset** on the device:  
Settings → System → Reset → Factory data reset  
(or via recovery mode)
- After the reset, **no automatic enrollment or MDM registration** will be applied.

**Notes:**

- The device **remains physically tied to the reseller** until they remove it from their inventory.
- If you plan **to resell or transfer** devices, ask the reseller or distributor to remove the device from their reseller list.

Devices assigned through Zero-Touch **cannot be manually removed by end users** — only by administrators or resellers.

## Windows

### Microsoft Intune / Azure AD / Windows Autopilot

Official links: [Remove devices | Microsoft Learn](#)

Official links: [Remove your Windows device from Intune management | Microsoft Learn](#)

Official links: [Remove your iOS device from Intune | Microsoft Learn](#)

Official links: [Remove device from Intune Company Portal for Android | Microsoft Learn](#)

#### Procedure:

**Step 1:** Sign in to the Intune Admin Center

1. Open the website:  
<https://intune.microsoft.com>
2. Sign in with your **Microsoft administrator account**.

**Step 2:** Find the device

1. Navigate to:  
**Devices** → **All devices**
2. Search for the device by:
  - Device name
  - Serial number
  - Username
  - IMEI (for mobile devices)
3. Select the appropriate device from the list.

**Step 3:** Remove DFCL profiles (if present)

1. In the left navigation, go to:  
**Device Configuration** → **Profiles**
2. Find the **DFCL profile(s)** (e.g., "DFCL - BIOS Lockdown")  
→ These are configuration profiles that set UEFI/BIOS settings..
3. Remove assignment of these profiles from the device:
  - Open the profile
  - Remove **assignment** under "Assigned Groups"

**Step 4:** Remove device from Intune

1. Click the **"..." (More options)** or **"Delete" button** at the top.
2. Confirm the deletion in the dialog box.

#### Important:

- This step **removes the device from Intune** and **breaks MDM management**.
- On the next device sync, **all MDM policies and configurations will be cleared**.

**Step 5:** Check and remove Azure AD registration

1. Open the **Microsoft Entra Admin Center** (formerly Azure AD):  
<https://entra.microsoft.com>

2. Go to:  
**Identities** → **Devices** → **All devices**
3. Find the device and select “Delete” to remove it from Azure AD as well.

**Step 6:** Remove device from Windows Autopilot (if registered)

1. In the **Intune Admin Center**, go to:  
**Devices** → **Windows** → **Windows enrollment**
2. Select **devices** under **Windows Autopilot Deployment Program**.
3. Search for the device (e.g., by serial number).
4. Check the box and click “**Delete**”.

**Important:** OEM Devices and Tenant Lock

- Devices shipped with an OEM Autopilot profile (e.g., directly from manufacturer or reseller) may be linked with a “Tenant Lock”.
- The hardware hash is assigned to a fixed tenant ID in Microsoft, regardless of removal from Intune or Azure AD.
- This means:  
Even after resetting and removing from Intune/Azure AD, the device may reconnect to the original tenant, especially once it regains internet access.
- Solution:  
The original tenant administrator (e.g., reseller or supplier) must open a support ticket with Microsoft to unlink the Autopilot device from the Tenant.
- Without this, **the automatic tenant assignment remains**.

**Step 7:** Reset the device

- **Factory reset** the device:
  - Android/iOS: Settings → Reset
  - Windows: Settings → System → Recovery → Reset this PC
- After reset, **no MDM enrollment will be active**.

**Additional notes:**

- A device **must be removed from both Intune and Azure AD** to be fully released.
- Some devices **automatically re-enroll in Intune** when reconnecting with the same account – check Autopilot/enrollment settings.
- Windows devices registered via **Autopilot** may **require removal of the Autopilot profile** as well.

## Other (combinations possible)

### VMware Workspace ONE (AirWatch)

#### Procedure:

##### Step 1: Log in

1. Open your Workspace ONE console
2. Log in with your admin account

##### Step 2: Find the device

1. Navigate to: **Devices** → **List View**
2. Search by device name, user, or serial number
3. Click on the affected device

##### Step 3: Delete the device

1. Click **"More Actions"** → **"Delete Device"** in the top right
2. Optional: Select **"Enterprise Wipe"** beforehand to remove the MDM profile
3. Confirm your selection

##### Step 4: Reset the device

- Manually perform a factory reset on the device
- Afterward, the device will no longer be assigned to MDM

### MobileIron / Ivanti Neurons for MDM

#### Procedure:

##### Step 1: Log in

1. Log in to Ivanti as an admin

##### Step 2: Search for the device

1. Go to **Devices** → **Search**
2. Locate the device using name, user, IMEI, etc.

##### Step 3: Delete the device

1. Select the device → **Actions** → **Delete** (for complete removal)

##### Step 4: Factory reset

- Manually reset the device (iOS/Android/Windows)
- The device will no longer be assigned to MDM

### Cisco Meraki Systems Manager

#### Procedure:

**Step 1:** Log in

1. Log in to the Meraki Dashboard
2. Select your network / location

**Step 2:** Find the device

1. Go to **Systems Manager** → **Monitor** → **Clients**
2. Search by serial number, device name, or user

**Step 3:** Remove the device

1. Select the device → Click the **trash icon (Delete)**  
Or: **More** → **Remove from Network**

**Step 4:** Reset

- Manually factory reset the device

## **SOTI MobiControl**

**Procedure:**

**Step 1:** Log in

1. Log in to the SOTI console

**Step 2:** Find the device

1. Go to **Devices** → Search by serial number, IMEI, or user

**Step 3:** Delete the device

1. Right-click on the device → **Delete**
2. Alternatively: **Unenroll Device**

**Step 4:** Reset the device

1. Perform a factory reset via the device or through a remote command

## **Jamf Cloud MDM**

**Procedure:**

**Step 1:** Log in to Jamf

1. Open the Jamf web console in your browser
2. Log in with your administrator account

**Step 2:** Search for the device

1. Navigate to **Devices** or **Computers** (depending on device type)
2. Search for the device you want to remove using:
  - Device name
  - Serial number
  - Username

**Step 3:** Select the device

1. Click the device name to open the detail view

**Step 4:** Unenroll the device

**Option A:** Erase the device remotely

1. Click **Management** or **Management Commands**
2. Select **Erase Device** or **Remove MDM Profile** (depending on platform and available commands)
3. Confirm the command

The device will be reset and removed from Jamf management

**Step 5:** Verify removal

- Check the device overview to confirm the device is removed
- The device should no longer receive MDM profiles or apps

**Important notes:**

- A **remote erase** will fully reset the device to factory settings
- Only removing the device in Jamf removes it from management but does not erase its data
- Devices managed via **DEP (Apple Device Enrollment Program)** may automatically re-enroll after reset if still assigned in the DEP portal

**Meta Quest (Meta for Business / Meta Workplace)**

**Procedure:**

1. Log in to your MDM system (e.g., Microsoft Intune portal)
2. Search by the serial number or name of the Meta Quest device
3. Click the relevant device in the device list
4. Choose **“Delete Device”, “Remove Device”, or “Retire Device”**
5. Confirm the removal from management
6. Perform a factory reset on the headset  
On the headset: Hold **Power + Volume Down**, then select **Factory Reset**  
Alternatively, in the Meta app under device settings → **Factory Reset**
7. After the reset, the device is no longer managed by MDM and can be set up again

**PICO Business MDM**

**Procedure:**

1. Open the Business Portal  
Go to <https://business.picoxr.com>
2. Log in with your administrator account
3. Navigate to the **Device Management** section
4. Search for the device by serial number or name
5. Click on the device you want to remove
6. Select **“Remove from fleet” or “Unregister”**
7. Confirm the action

8. Factory reset the PICO headset  
Go to: **Settings** → **General** → **Factory Reset**  
Or: Hold **Power + Volume Down**, then select **Factory Reset**
9. After the reset, the device is no longer bound to MDM and can be reconfigured

## **HTC VIVE Business MDM**

### **Procedure:**

1. Open the Business Portal  
Go to <https://business.vive.com>
2. Log in with your administrator account
3. Navigate to the **Devices** or **Device Management** section
4. Locate the device using the serial number or device name
5. Click on the desired device
6. Select **"Remove device"** or **"Unregister"**
7. Confirm the removal
8. Perform a factory reset on the headset  
Go to: **Settings** → **General** → **Factory Reset**  
Or: Hold **Power + Volume Down**, then select **Factory Reset**
9. After the reset, the device is free from MDM locks and can be re-enrolled

### **General Notice**

The information provided in this guide is based on the currently valid requirements and processes, including the specifications of the respective manufacturers. Please note that manufacturer requirements and information are subject to change at any time. CHG-MERIDIAN assumes no liability for the completeness or timeliness of the information provided, as changes and/or additions made by the manufacturers may not be immediately reflected in this guide. We recommend that our customers contact us or the manufacturer directly if they have specific questions or uncertainties.