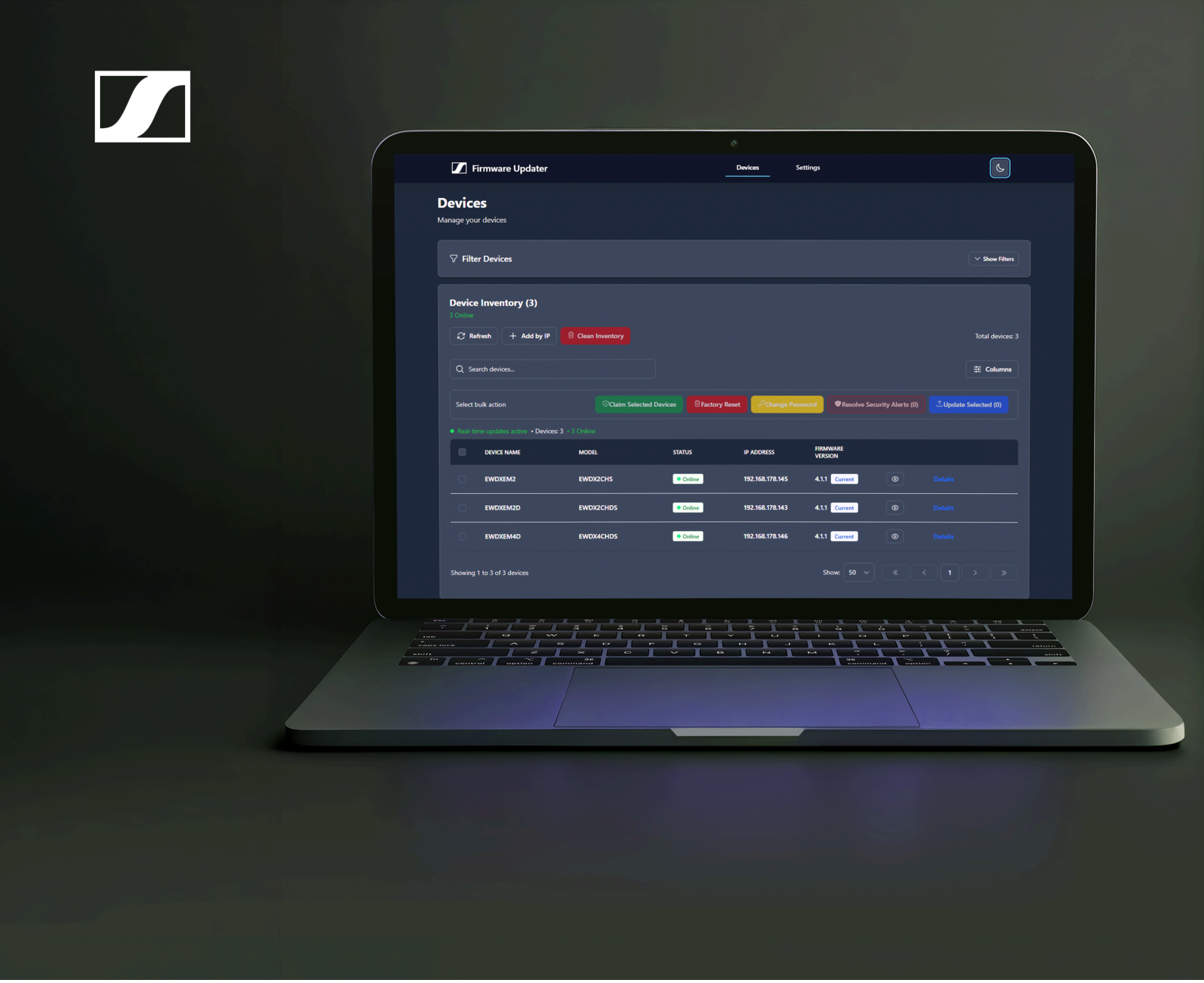


Firmware Updater

Device management for audio equipment

PDF export of the original HTML manual

Contents

1. Preface ... 3
2. Product information ... 4
3. Get started ... 6
    Installing the software ... 6
    Starting the software ... 9
    Enabling/disabling data collection ... 10
    Toggle themes ... 11
4. Instruction manual ... 12
    Device inventory ... 12
        Using search ... 14
        Using filters ... 15
        Setting the page size ... 16
        Cleaning up the inventory ... 17
    Adding devices ... 18
    Claiming devices ... 20
    Bulk device operations ... 22
        Bulk device claiming ... 22
        Bulk firmware updates ... 25
        Bulk password changes ... 28
        Bulk factory resets ... 30
    Updating devices ... 32
        Offline firmware updates ... 34
    Changing the password ... 35
    Factory reset ... 37
        Resetting the L6000 charger ... 38
    Resolving security certificate warnings ... 39
5. Knowledge base ... 40
    FAQ ... 40

1. Preface

PDF Export of the Original HTML Manual

This PDF document is an automatic export of an interactive set of HTML manuals. Some content and interactive elements may not be included in the PDF because they cannot be displayed in this format. In addition, automatically generated page breaks may cause related content to be slightly shifted. We can therefore only guarantee the completeness of the information in the HTML manual and recommend using it. You can find it in the Documentation Portal at www.sennheiser.com/documentation.

2. Product information

Information about supported devices, requirements and the main features of the software at a glance.

Key features

The Firmware Updater is a comprehensive device management solution designed for audio professionals who need efficient, reliable equipment management. It provides four core capabilities: updating device firmware, claiming devices for management, changing device passwords, and performing factory resets.

- Version 1.3.0 adds bulk operations across entire device fleets, native macOS support, and L6000 charger management — letting rental technicians prepare returned equipment in a fraction of the time previously required.
- Version 1.3.1 is a maintenance release that improves the stability and reliability of the application. The feature set is unchanged compared to version 1.3.0.

Technical requirements

Requirement	Windows	macOS
Operating system	Windows 11	macOS Ventura, macOS Sonoma, or macOS Sequoia
Runtime	.NET 8 SDK (.NET 8 Runtime & ASP.NET 8 Runtime, detected automatically by the installer; a download link is provided if not present)	.NET 8 SDK (.NET 8 Runtime & ASP.NET 8 Runtime, detected automatically by the installer; a download link is provided if not present)
Processor	—	Apple Silicon (M-series) only
Memory	4 GB RAM minimum, 8 GB recommended	4 GB RAM minimum, 8 GB recommended
Network / browser	Ethernet or Wi-Fi connectivity, same subnet as managed devices; modern web browser for web-based interface (Chrome 90+, Firefox 88+)	Standard network ports: HTTP/HTTPS (80/443), mDNS (5353), SSCv1 (45, UDP)

Network requirements

- IPv4 network connectivity
- DHCP support (recommended)
- Multicast DNS (mDNS) support for automatic discovery
- Standard network ports: HTTP/HTTPS (80/443), mDNS (5353), SSCv1 (45, UDP)

Supported devices

- EW-DX series devices with network management capabilities
- L6000 chargers (new in this release)

3. Get started

Detailed description of the installation, start-up and an overview of the software.

Installing the software

The Firmware Updater is available for Windows and macOS.

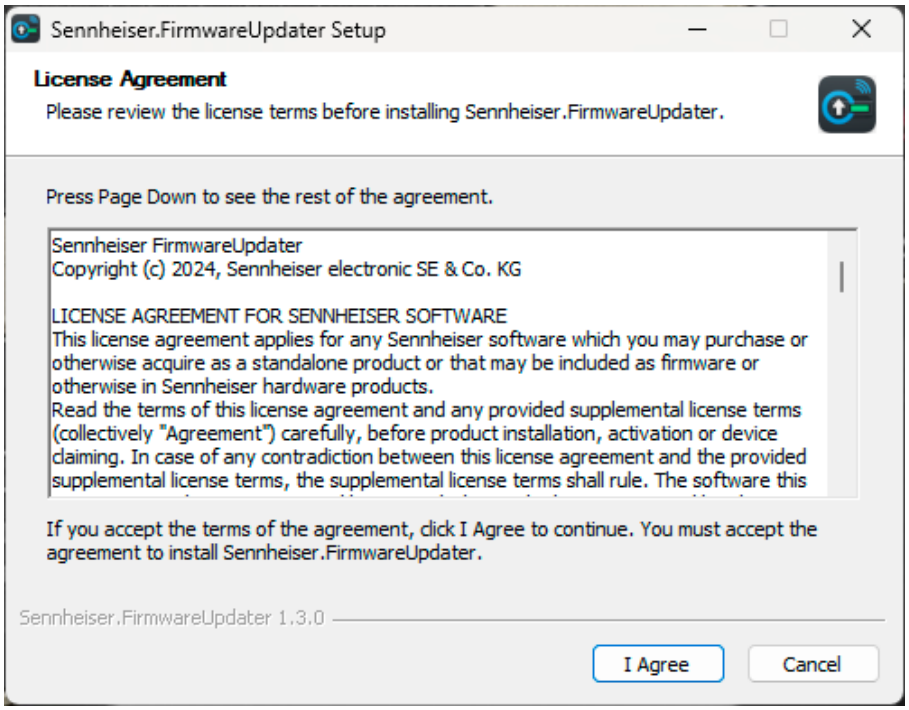
The installer detects whether the required .NET 8 runtime is present and provides a download link if it is not.

To install on Windows:

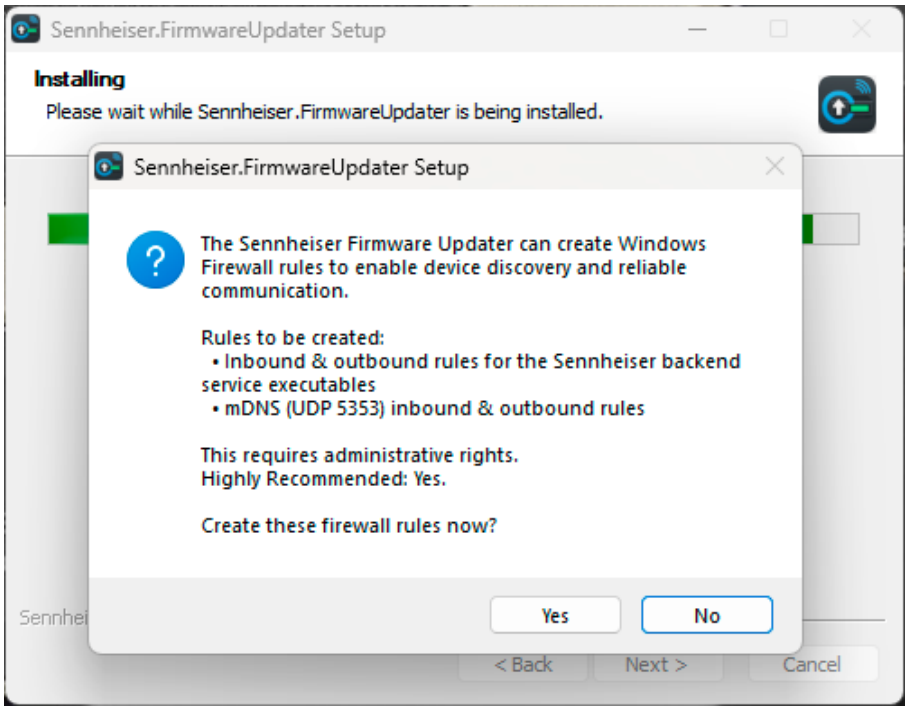
- Navigate to the product page.
- Accept the terms and conditions.
- Click on **Download**.

To install the Firmware Updater:

- Double-click on the downloaded software.
  - The installer is digitally signed - you won't see security warnings during installation.
- When prompted, accept the license agreement to proceed with installation.

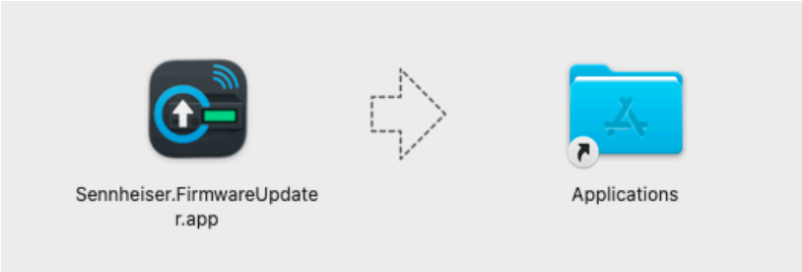


If requested, allow the installer to configure the Windows Firewall rules for device discovery (mDNS / UDP port 5353).

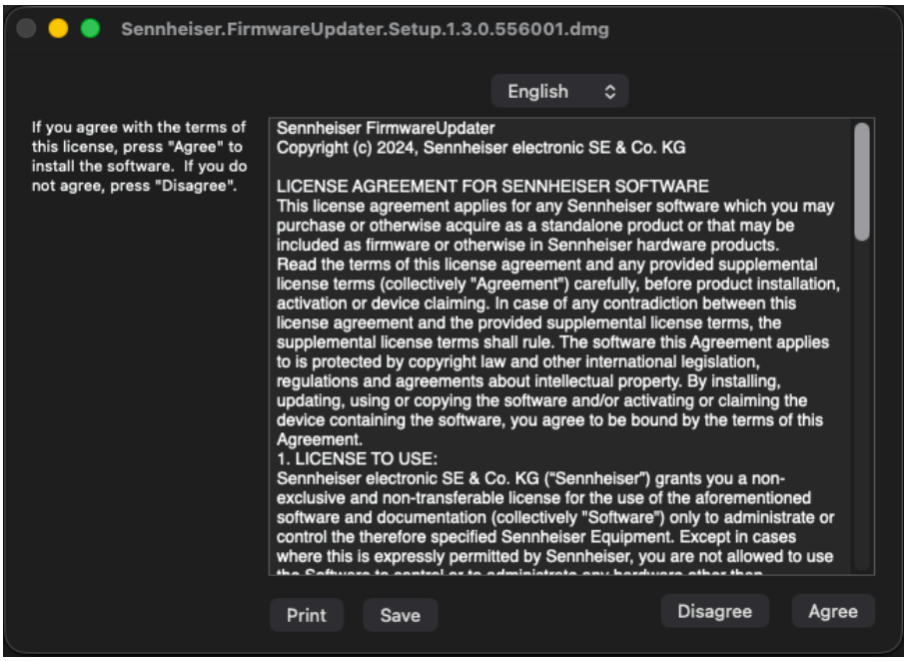


To install on macOS:

- Download the macOS installer, delivered as a **DMG** file.
- Open the DMG and drag the application into the **Applications** folder.



- Launch the application. It is code-signed and notarized, so no security warnings appear during installation or launch.



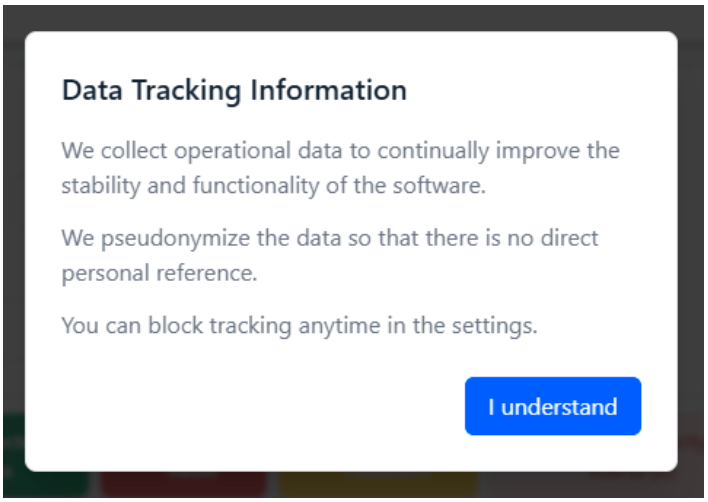
To uninstall on macOS, drag the application from the Applications folder to the trash.

✓ The software has been installed.

Starting the software

When you first open the Firmware Updater:

- A pop-up will inform you that we collect operational data to improve software stability and functionality.
- The data is pseudonymized so there is no direct personal reference.
- You can block tracking anytime in the settings (see Enabling/disabling data collection).
- Close the pop-up to continue to the main interface.



✓ You have successfully started the software.

Enabling/disabling data collection

The Firmware Updater collects operational data to improve stability and functionality.

What we collect:

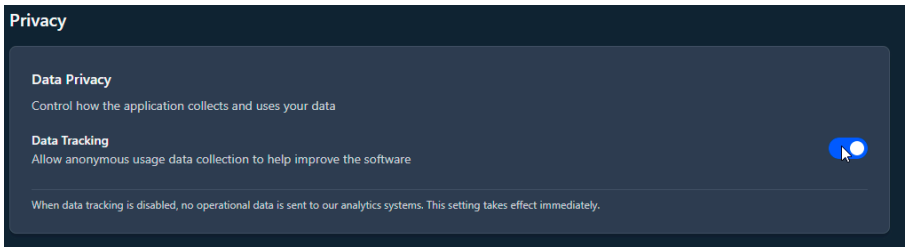
- Anonymized usage information
- No personally identifiable information
- Data is pseudonymized (no direct personal reference)
- Used only for software improvement

When data collecting is blocked:

- No operational data is sent to our systems
- All software functionality remains available
- Your choice is respected and maintained

To enable/disable data collection:

- Go to **Settings** > **Privacy**.
- Toggle **Data Tracking**.



  - The changes apply immediately and remain after restarting the application.

Data collection has been enabled/disabled.

Toggle themes

You can switch between light and dark themes, using the toggle located in the top right corner.

The following options are available:



Dark Mode

- Reduces eye strain in low-light environments.
- Optimized for nighttime and dimly lit work areas.



Light Mode

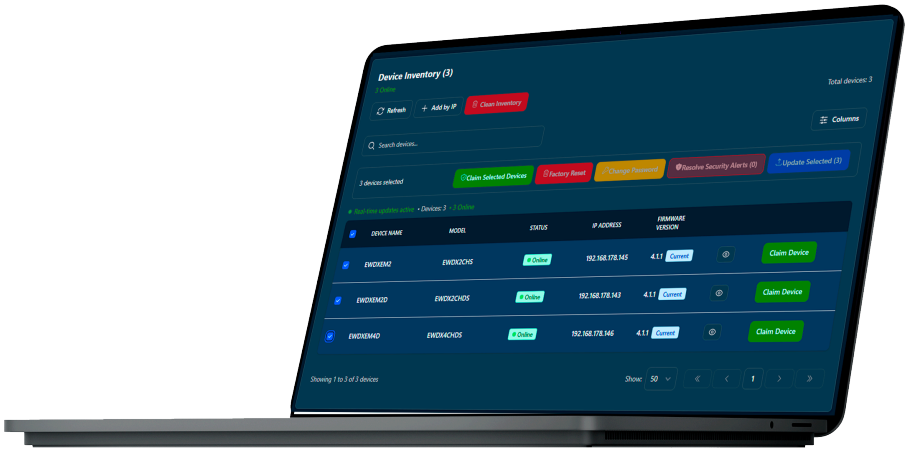


System Settings

The changes apply immediately and remain after restarting the application.

4. Instruction manual

Detailed description of how to start the software and configure your devices.



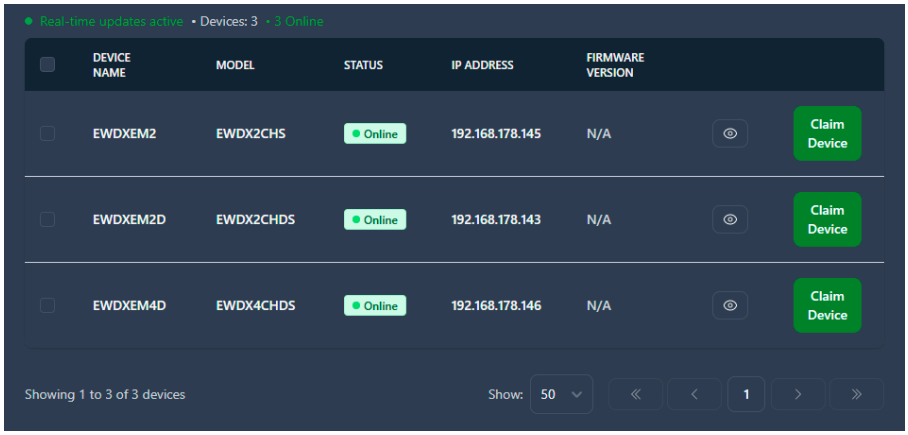
This manual covers all functionality available in the 1.3.0 release. For additional support, please contact our technical support team or submit a request at at help.sennheiser.com/request.

Device inventory

The main device inventory view shows all your discovered and manually added devices in one place.

Information displayed

- Device name and type
- Connection status
- Current IP address
- Firmware version

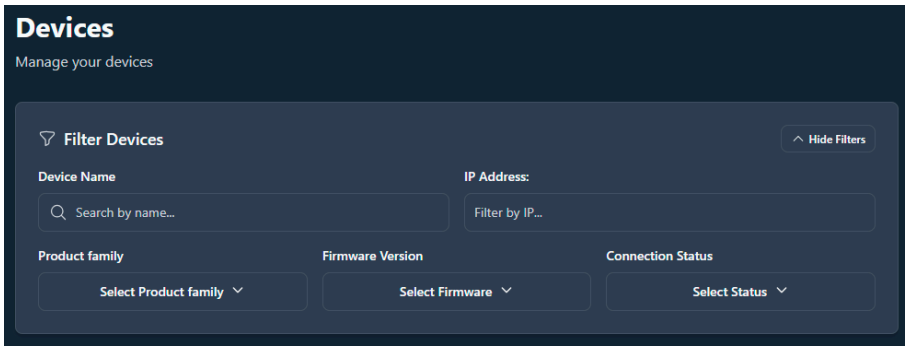


> The view updates in real-time when device states change.

Search and filter

Find specific devices quickly by using search and/or filters:

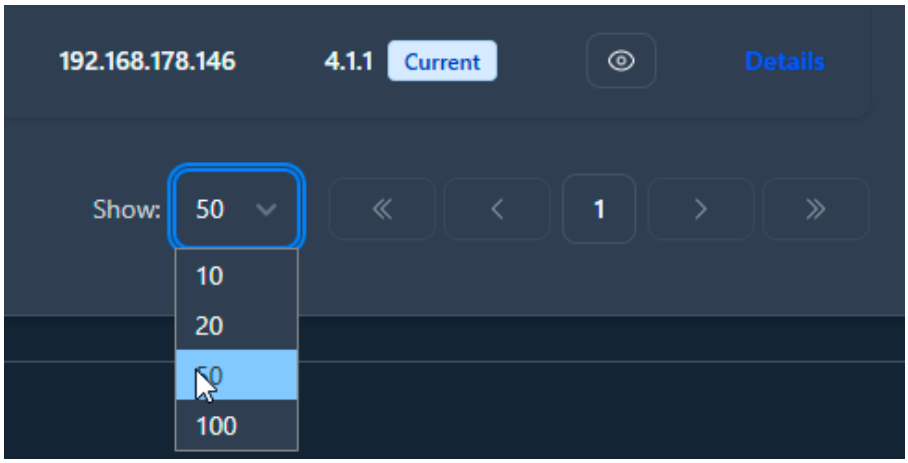
- Search, see Using search
- Filters, see Using filters



Pagination

For large device inventories:

- Page sizes, see Setting the page size
    - You can change the number of devices shown in the inventory.
- Navigation
    - Use Next/Previous buttons to navigate pages
    - Jump to first or last page directly
    - Changing page size takes you back to the first page



Using search

You can search for added devices by name or ID.

You can use partial keywords - e.g., entering **RX** finds all receivers.

The search is case-insensitive.

To find a device:

- Type in the name or the ID.

✓ The search result is shown.

Using filters

You can filter the displayed devices.

The following filters are available:

- Product family
- Firmware version
- IP address
- Connection status

To use filters:

- You can select multiple filters at once (e.g., , product family AND firmware version).
  - The results update instantly as you apply the filters.

To reset the filters:

- Click **Clear All** to reset all filters.
  - All filters have been cleared.

✓ The devices have been filtered.

Setting the page size

For large device inventories, adjust the page size to display more devices at once.

- Default: 20 devices per page
- Options: 10, 20, 50, or 100 devices per page

The changes remain after restarting the application.

To change the page size:

▶ Choose your preferred page size.

✓ The page size is saved automatically and remains after restarting the application.

> **i** Changing the page size will take you back to the first page.

✓ The page size has been changed.

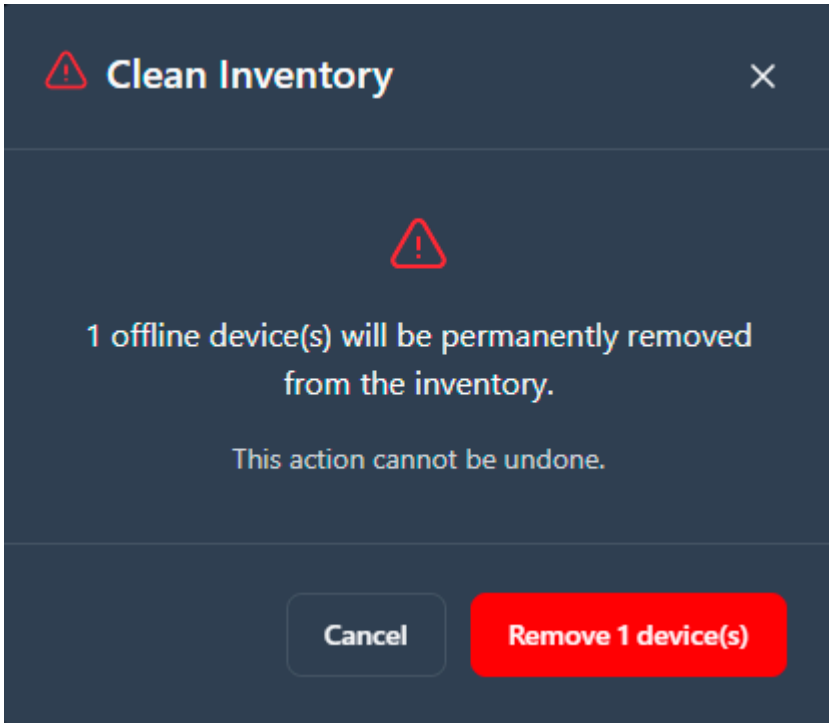
Cleaning up the inventory

You can remove all offline devices from the inventory in a single action.

Removing devices is useful for quickly clearing stale or disconnected devices between rental sessions.

To clean up the inventory:

- Click the **Clean Inventory**action.
- Confirm the removal of offline devices in the dialog.



The device inventory also refreshes automatically when the application window regains focus, so the displayed state is always current.

✓ All offline devices have been removed from the inventory.

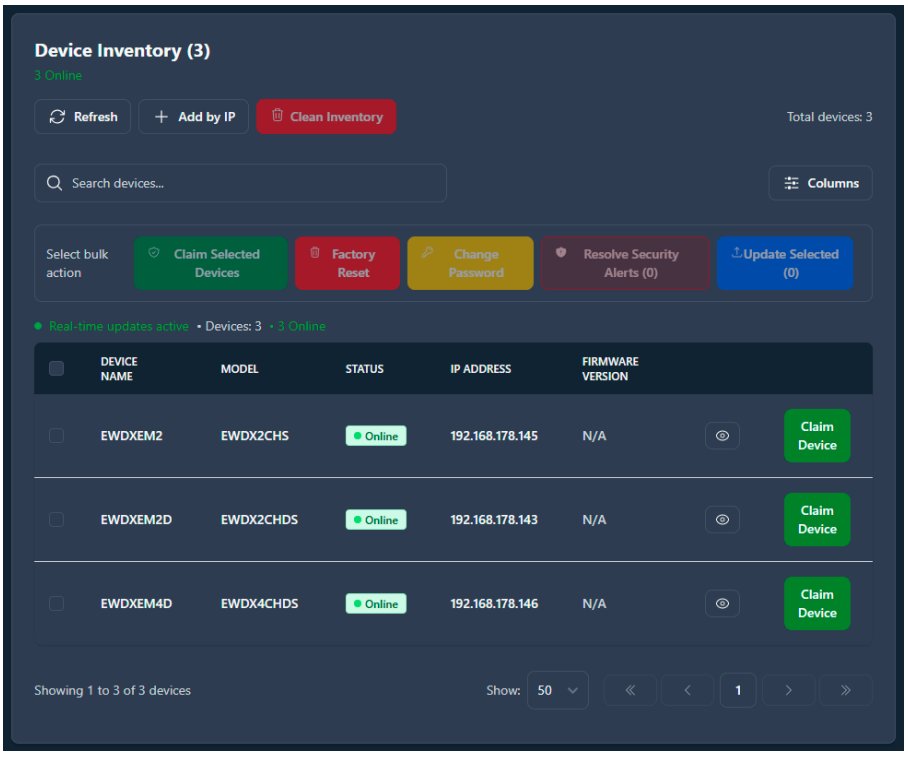
Adding devices

You can add devices automatically or manually.

The Firmware Updater automatically discovers devices in your network when you open the application.

To a add new device with Automatic Device Discovery:

- All discoverable devices are listed within 10 seconds of scanning.
- Devices show name, type, and IP address.
- The list updates automatically when devices join or leave the network.
- A manual refresh option is available if needed.



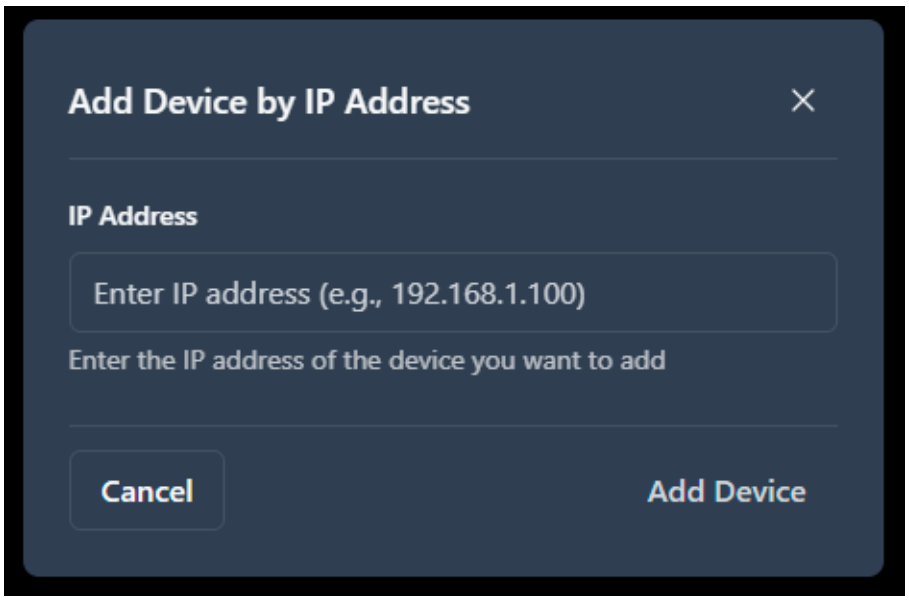
If no devices are found:

- A message will indicate no devices were found.
- Check that devices are powered on and connected to the same network.
- Try adding devices manually using their IP address.

To add a new device manually:

If devices don't appear automatically, you can add them manually.

- Click on **Add by IP**.
- Enter the device's IP address (e.g., 192.168.1.100).
- Click on **Add Device**.



What the system checks:

- Valid IP address format
- No duplicate IP addresses already in your list
- Device is reachable on the network

Error messages you might see:

- Device with this IP already exists
- Invalid IP format
- Device not reachable
- Connection timed out – please check the device or network

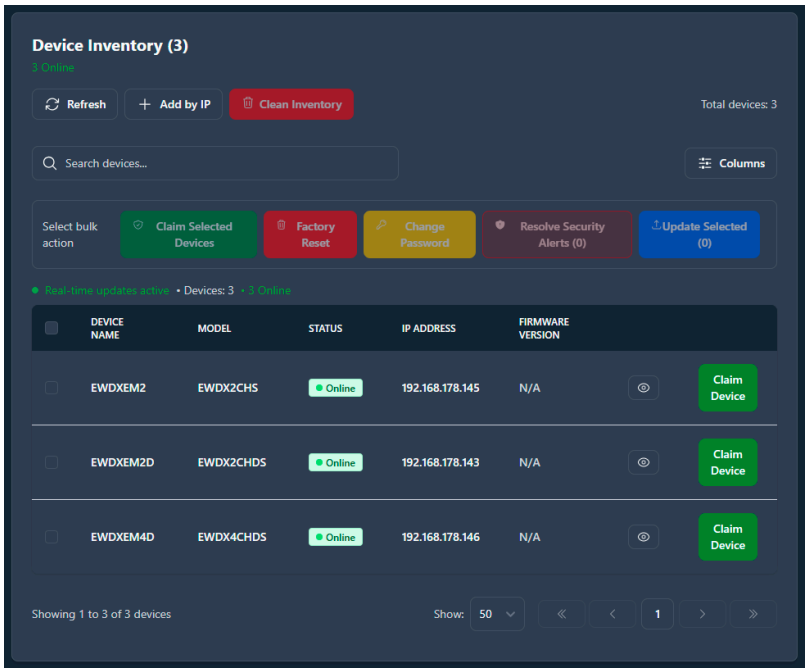
The device has been added.

Claiming devices

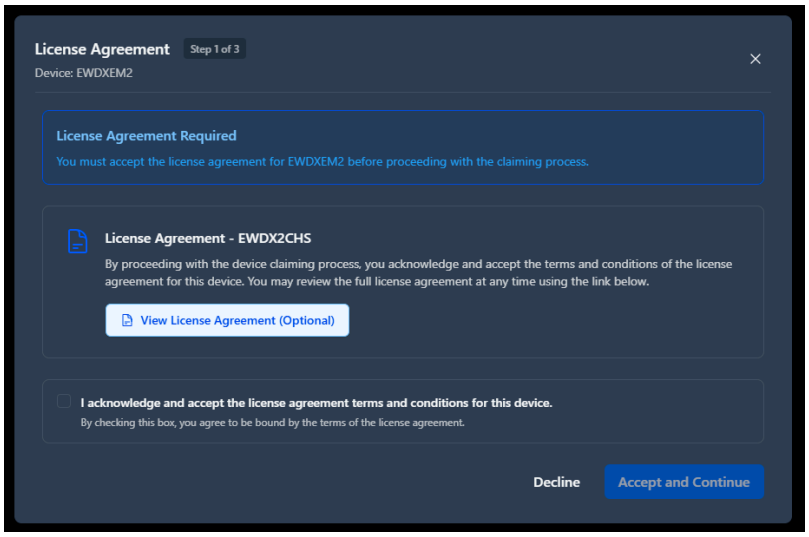
Before you can manage an EW-DX device, you need to claim it.

To claim a device:

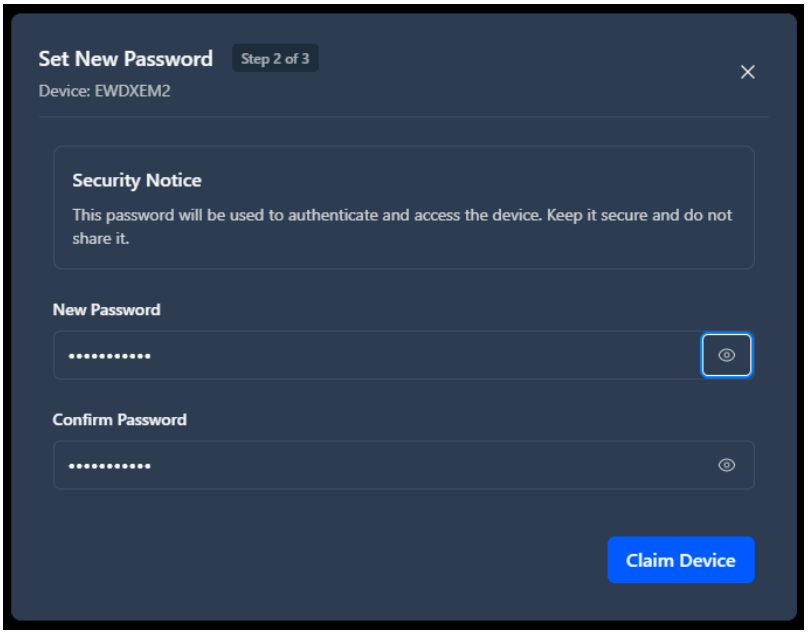
- Find the unclaimed device in the discovery list.
- Click on **Claim Device**.



- A modal will open asking to accept the license agreement terms and conditions for this device.



- After accepting click **Accept and Continue**.
- Enter and confirm a new password that meets the password requirements.



- Click to claim the device.
  - The device will then appear in your managed device list and you can configure it for your production.

✓ The device has been claimed.

Bulk device operations

Rental technicians can now prepare entire device fleets in a single workflow.

Operations overview:

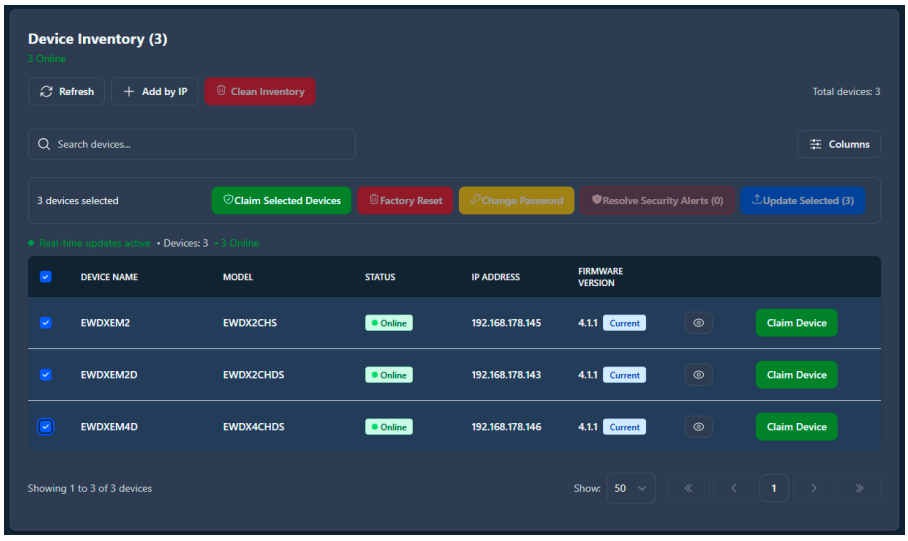
- Bulk device claiming
- Bulk firmware updates
- Bulk password changes
- Bulk factory resets

All bulk operations support 2–80 devices simultaneously and require no more than 3–4 clicks from selection to completion. Failed operations are automatically retried once before being flagged for individual attention, and a post-operation summary gives a clear overview of the results.

> **i** Devices that are not eligible for a selected bulk operation are silently excluded from that action; the results summary shows exactly which devices were affected.

To select multiple devices:

- Use the selection checkboxes in the device inventory to select the devices you want to act on.
- Choose the bulk action to perform (claim, update, change password, or factory reset).



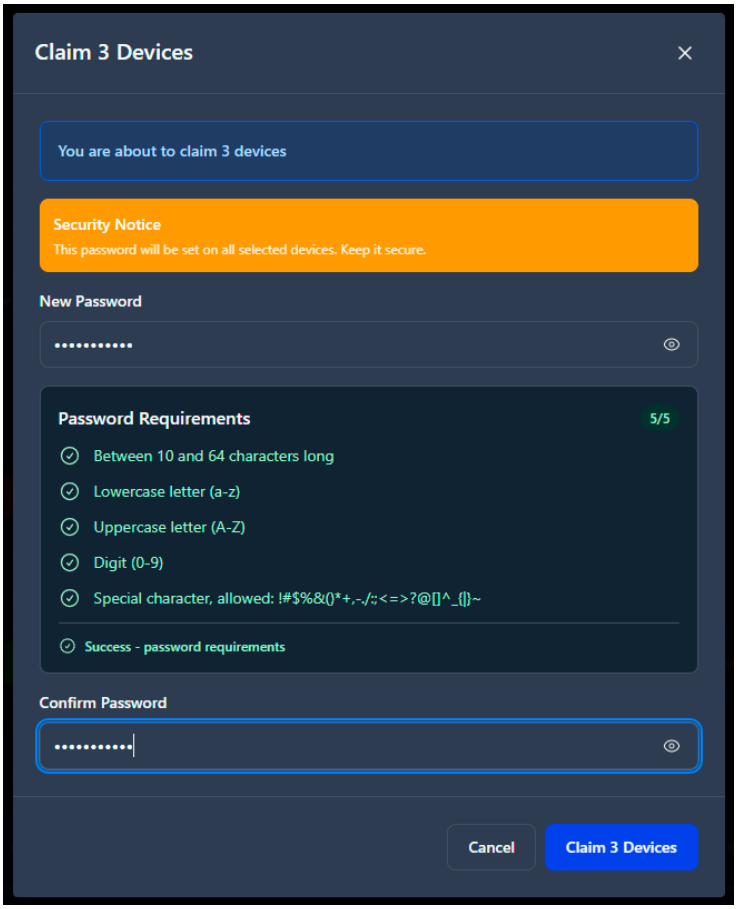
Bulk device claiming

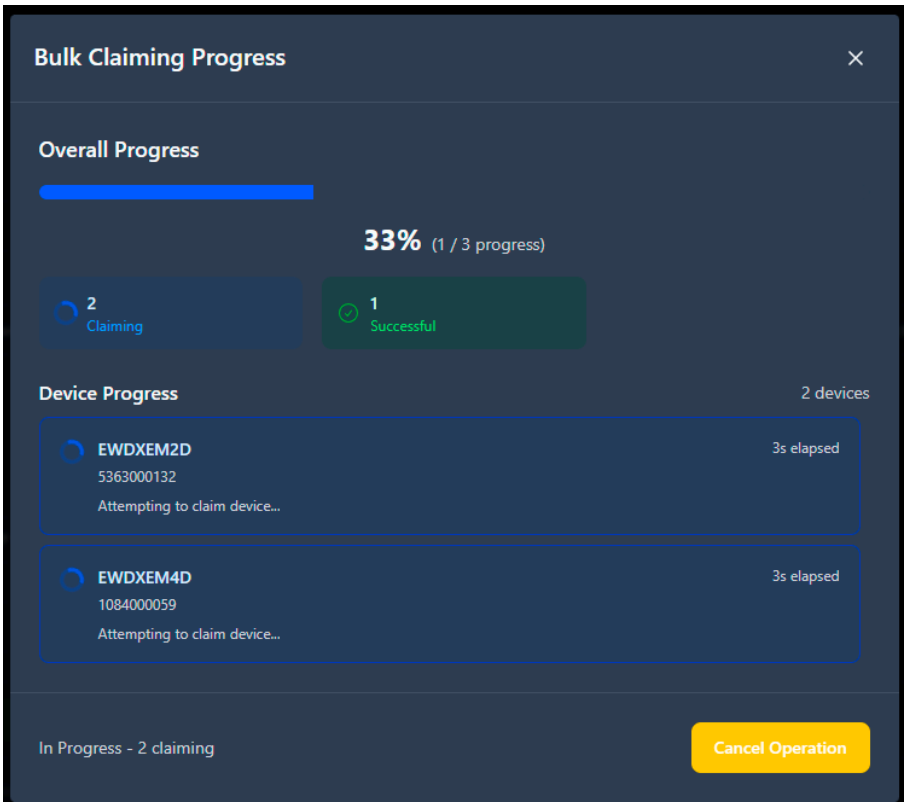
Select multiple unclaimed devices and claim them with a single password entry.

Claiming runs in parallel. Each device shows its own live progress indicator.

To claim bulk devices:

- Select the unclaimed devices you want to claim.
- Start the claiming process.
- Enter the password once for all selected devices.





Failed claims show specific error messages. Retry each failed device independently.

You have successfully claimed the devices.

Bulk firmware updates

Select multiple claimed devices and update their firmware at the same time.

When you use locally uploaded firmware files, select a specific firmware version for each product model before the update starts. This gives you precise control over mixed-model fleets.

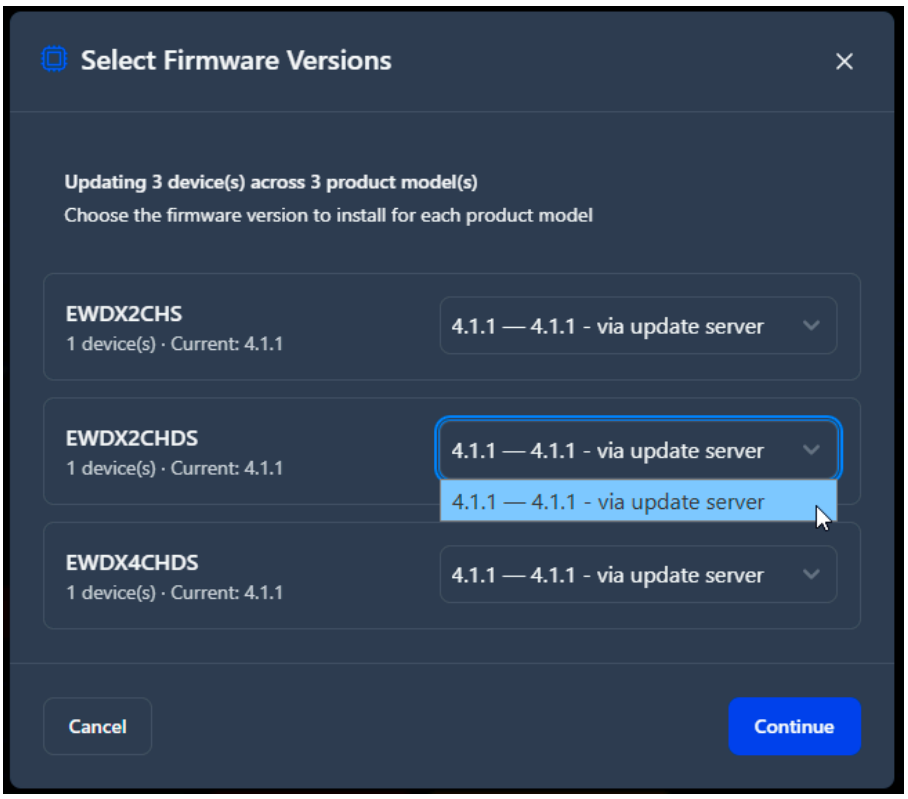
The validation summary shows which devices need updates and which devices already run the current firmware.

Closing the application during active updates

- If you try to close the application while firmware updates are in progress, a confirmation dialog appears.
- The dialog lists the devices that are currently updating.
- Device-side updates continue after the application is closed. Closing the application does not interrupt or damage ongoing firmware updates.

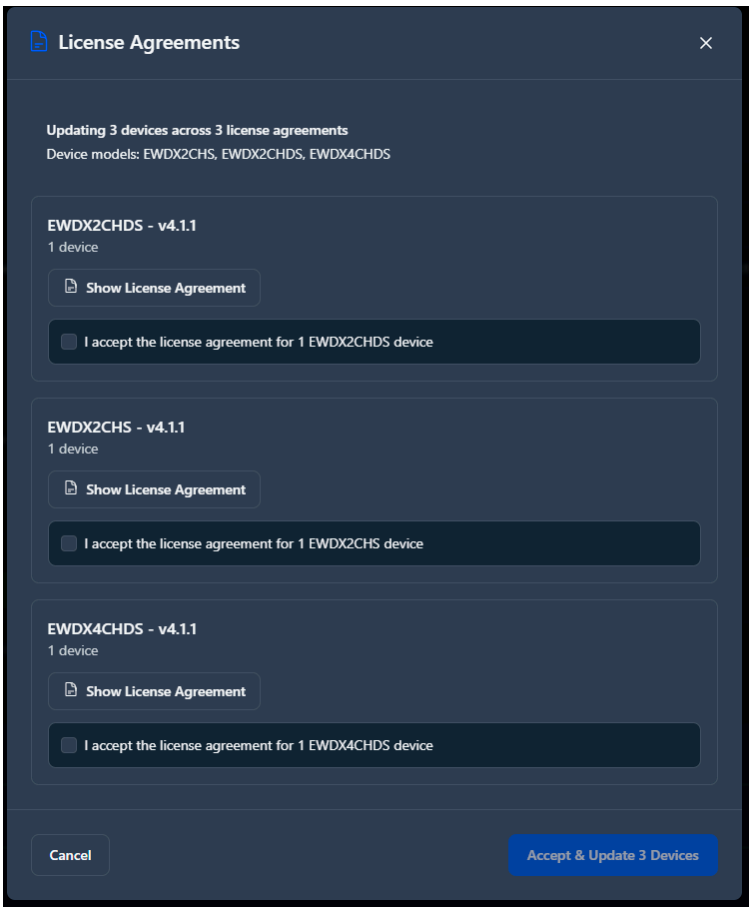
To update bulk devices:

- Select the firmware versions for the devices you want to update.



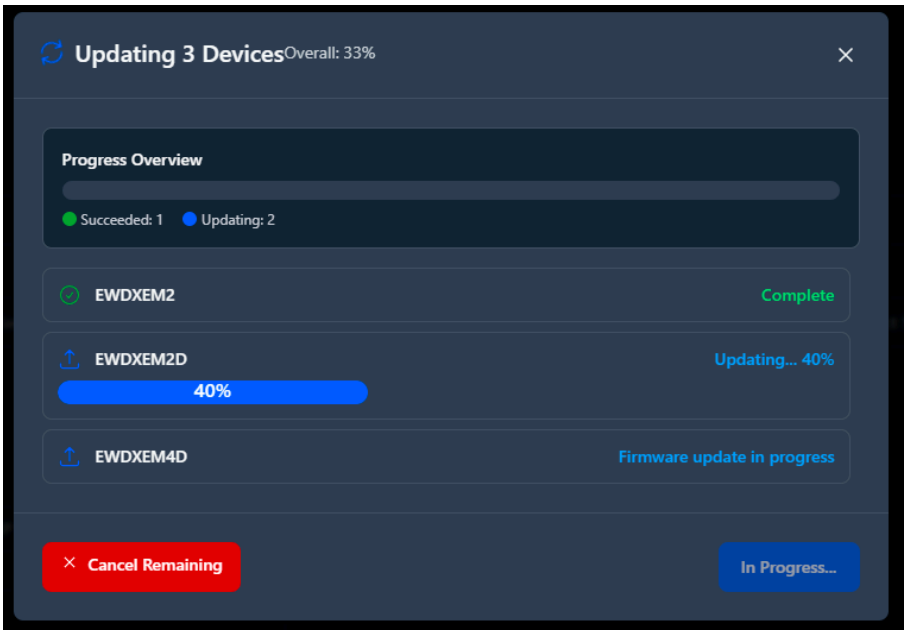
- Click **Continue** to start the update process.

- Review the validation summary and confirm the firmware versions for each product model if you use locally uploaded firmware files.



- Click **Accept & Update {number} Devices** to confirm the update and accept the license agreement for the full device batch.

  The download, installation, and verification progress is shown separately for each device. Failed updates are retried once automatically before manual intervention is required.



A single license agreement modal covers the full device batch before any update begins. The modal states how many devices are affected and cannot be bypassed. If you decline it, the entire batch operation is canceled and the device selection view is restored.

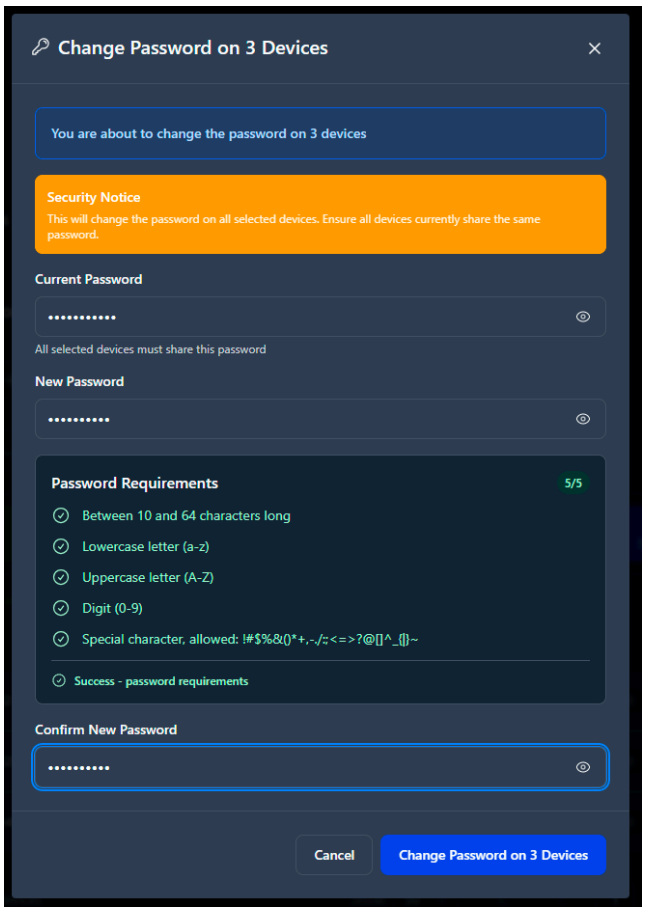
The bulk update has been completed successfully.

Bulk password changes

Apply a new password to multiple claimed devices in a single operation.

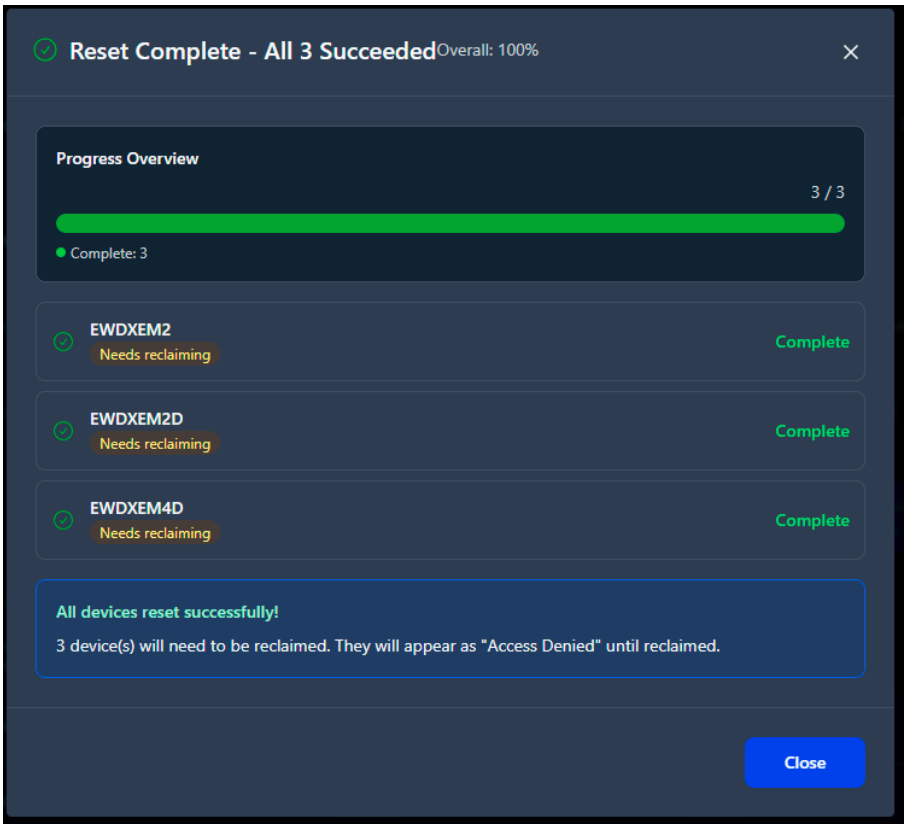
To change bulk passwords:

- Select the devices whose passwords you want to change.
- Click **Change Password on {number} Devices**.



Password strength is validated once before any device is updated.

Successful and failed devices are reported individually in the results summary.



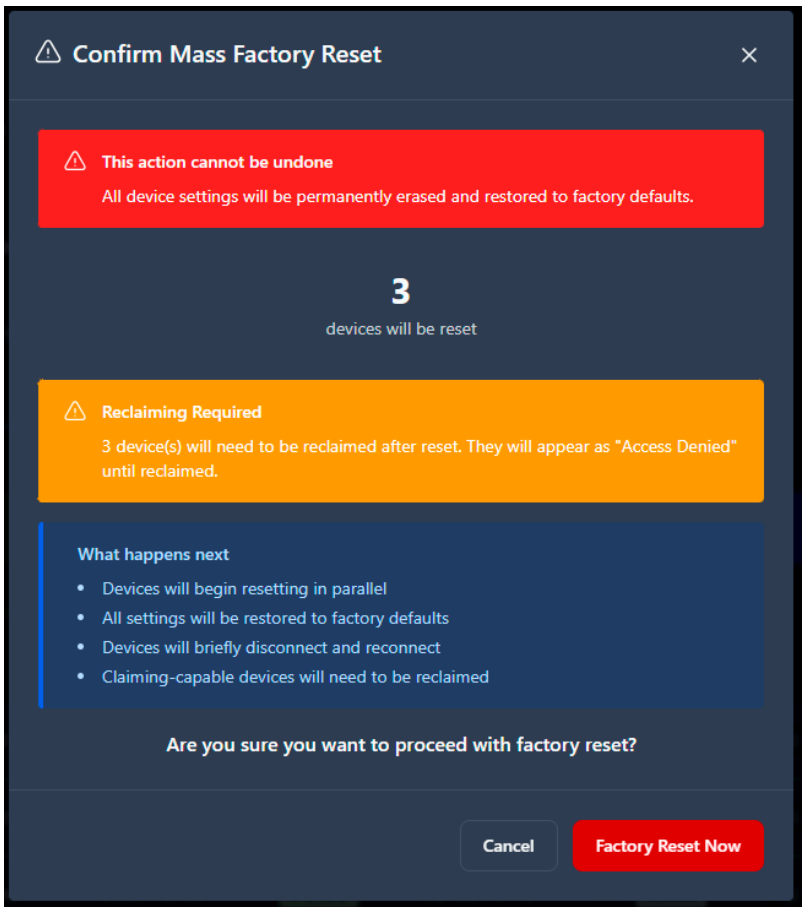
The bulk password change has been completed successfully.

Bulk factory resets

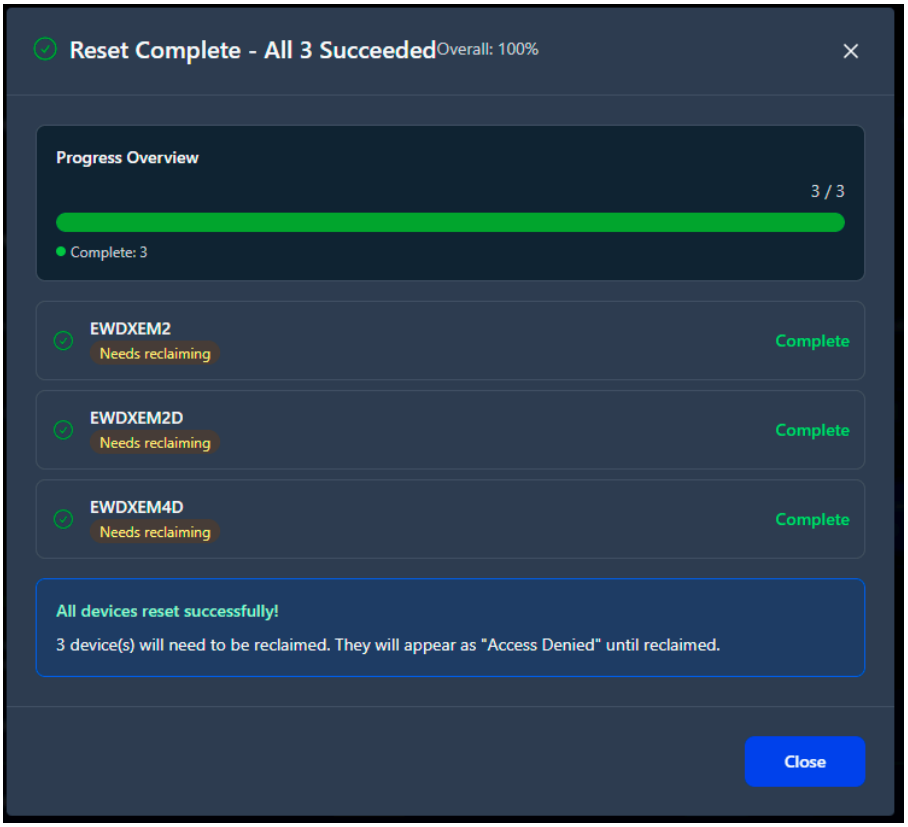
Reset multiple claimed devices to factory settings at the same time.

To reset multiple devices to factory settings:

- Select the devices you want to reset.
- Click **Factory Reset Now**.



A confirmation modal states that the devices will return to unclaimed status and lists all affected devices. Successfully reset devices reappear automatically in the device inventory as unclaimed.

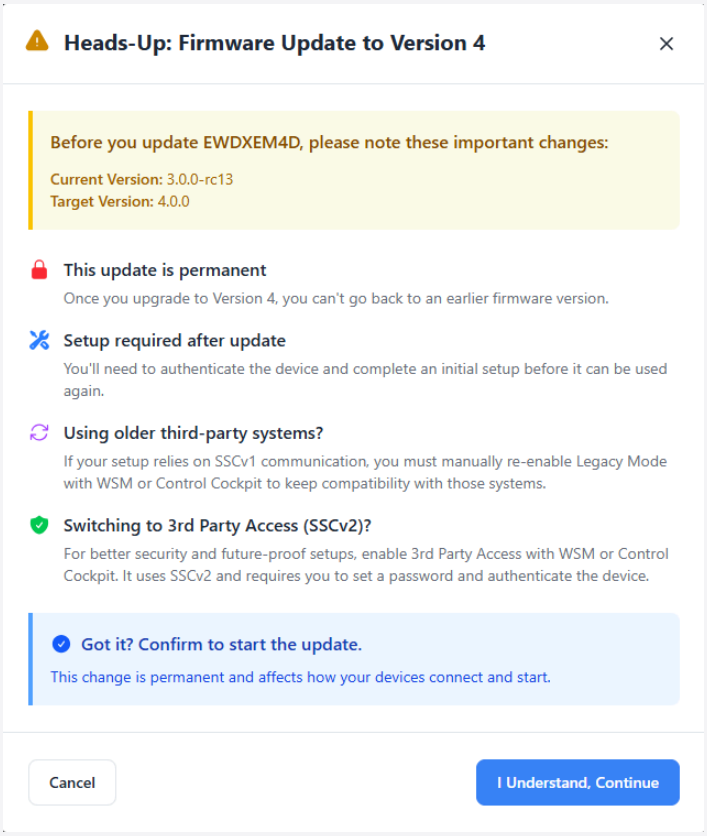


The bulk reset to factory settings has been completed successfully.

Updating devices

Updating from version 3.x to version 4.x
When updating a device from firmware version 3.x to version 4.x, you'll see a special warning modal explaining:

- This update is irreversible.
- You'll need to complete a required setup after the update.
- Legacy mode will be available for older protocol compatibility.
- SSCv2 will be activated for enhanced security.

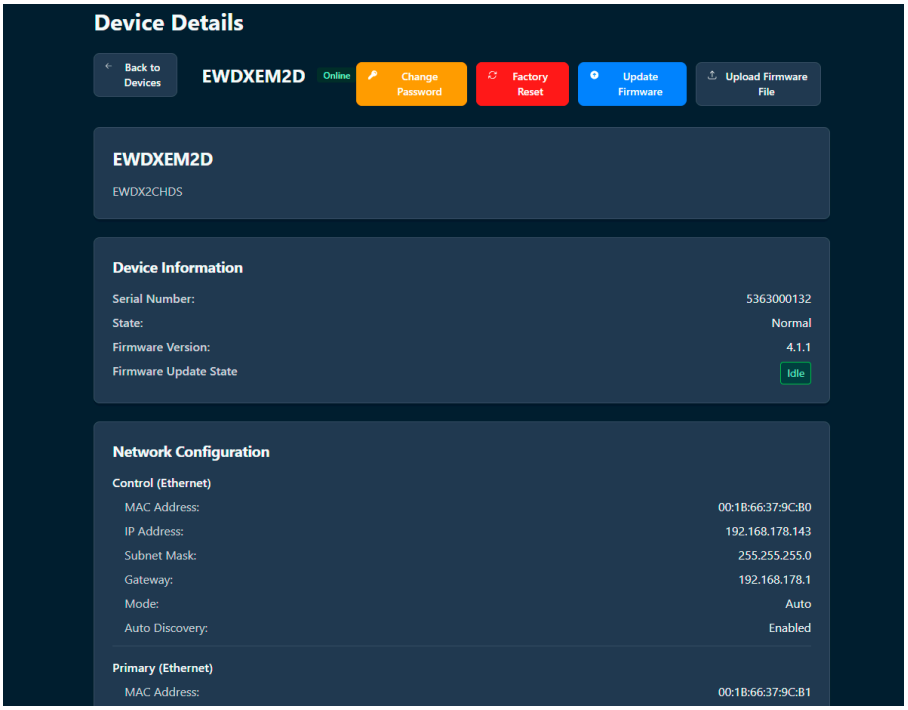


The update cannot start without license acceptance. You must acknowledge these points before the update can proceed. **License Agreements**
Every firmware update requires you to accept a license agreement. The license is shown before the update begins.

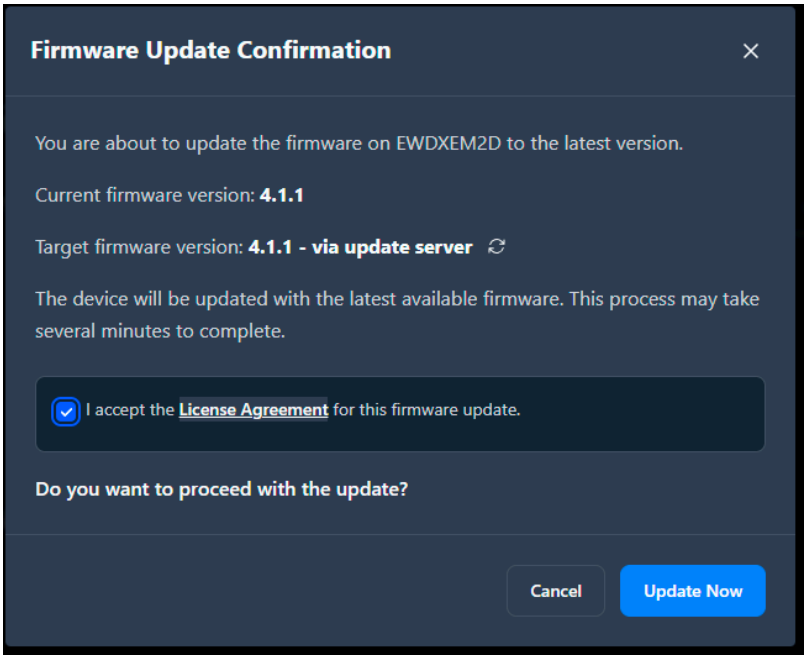
- You must click **Accept** to proceed.
- Click on **Cancel** in order to cancel the update.

To update a single device firmware:

- Open the device detail view.



- Click on **Update Firmware**.
- Accept the license agreement when prompted.



- The update begins with a progress indicator.

You'll see a success or failure message when complete.

✓ The device has been updated.

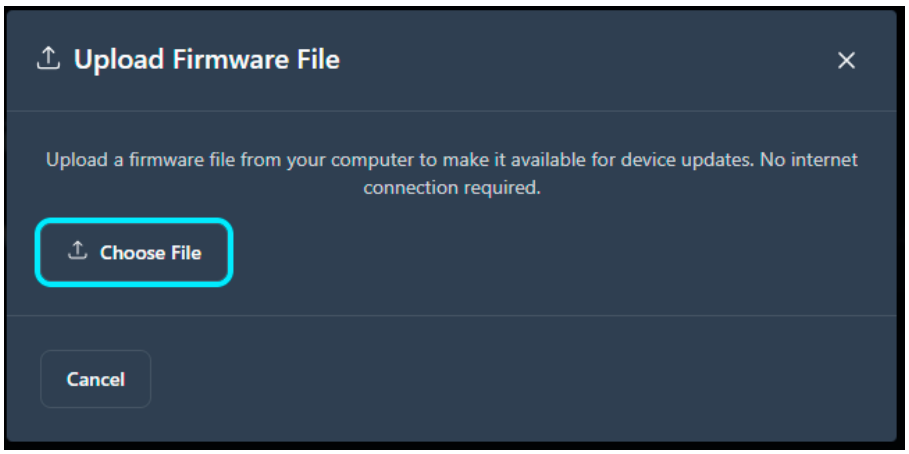
Offline firmware updates

Perform firmware updates from a local firmware image file when the device has no internet connection.

Firmware updates can be performed without an internet connection by using a local firmware image file. This is useful in venues with limited or no network access.

To update your firmware offline:

- Select a device and choose the option to update from a local firmware image file.
- Select the firmware image file.



  - The system validates file compatibility, including model, version, and checksum, before it applies the update.
- Monitor the update progress.
  - Success or failure feedback appears in the same way as for online updates. Incompatible files and interrupted transfers show clear error messages and retry options.

✓ Your device has been updated offline successfully.

Changing the password

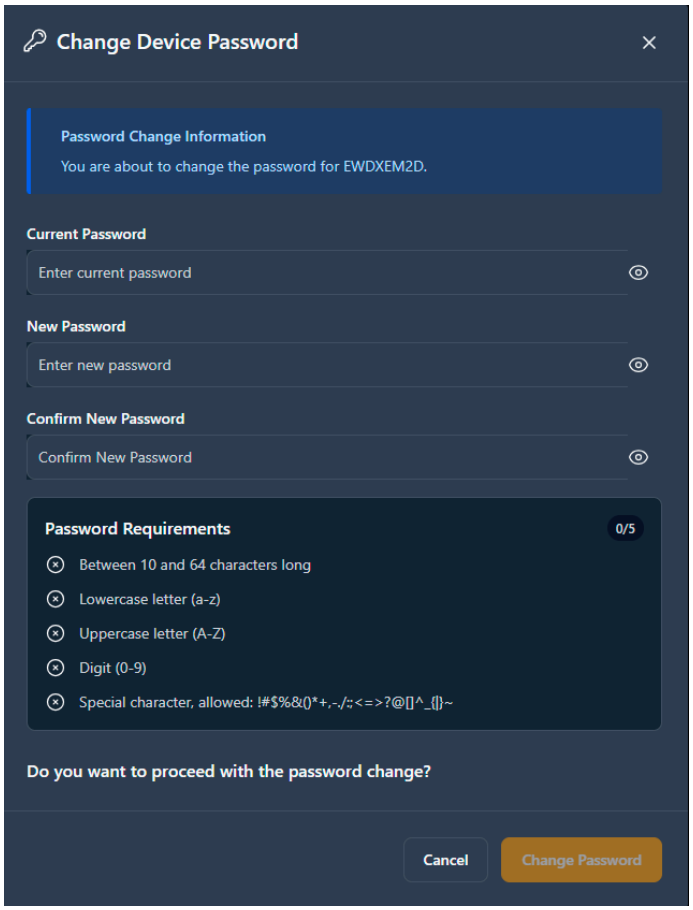
Change the device password quickly and securely.

To change the devices password:

- Open the device detail view.
- Click on **Change Password**.
- Enter your new password.

> Password requirements:
> - The system validates password strength in real-time
> - Weak passwords are not accepted
> - Success or failure feedback appears immediately
> - Changes take effect within seconds

- Confirm the password.
- Click on **Change Password** to save the change.



The password has been changed.

Factory reset

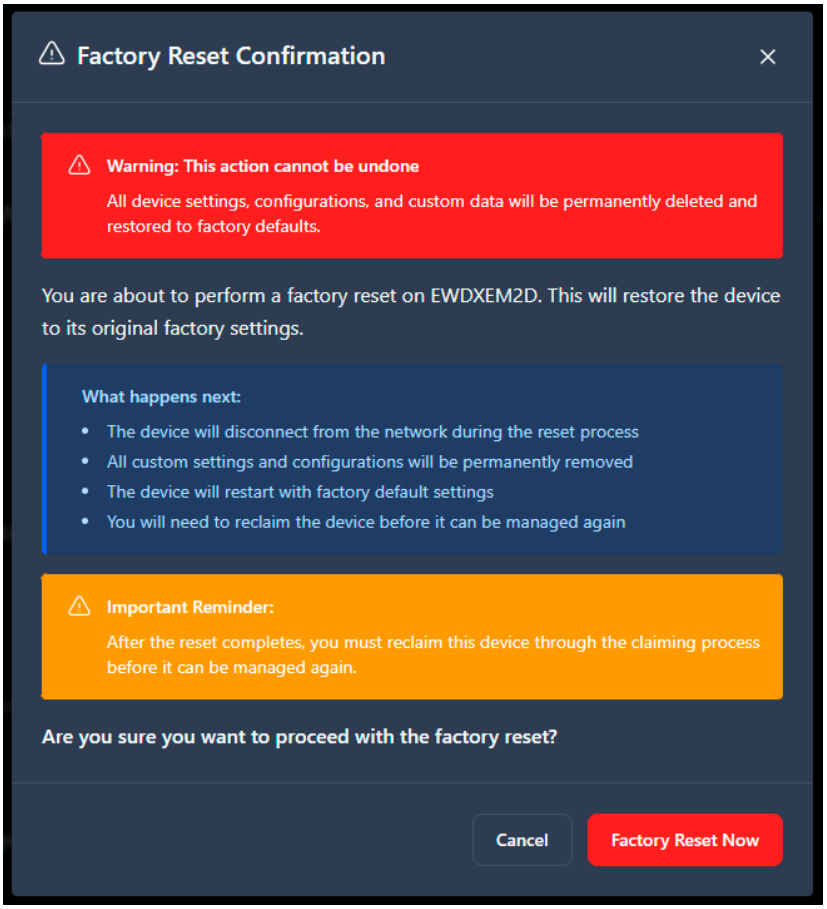
Reset devices to factory settings for rental turnaround.

Safety features:

- Confirmation required to prevent accidental resets.
- Reset button is disabled during firmware updates.
- Clear error messages if the reset fails.
- Progress tracking shows reset status.

To reset the device to the factory settings:

- Go to the device detail page.
- Click on **Factory Reset**.
- Confirm the reset in the dialog box.



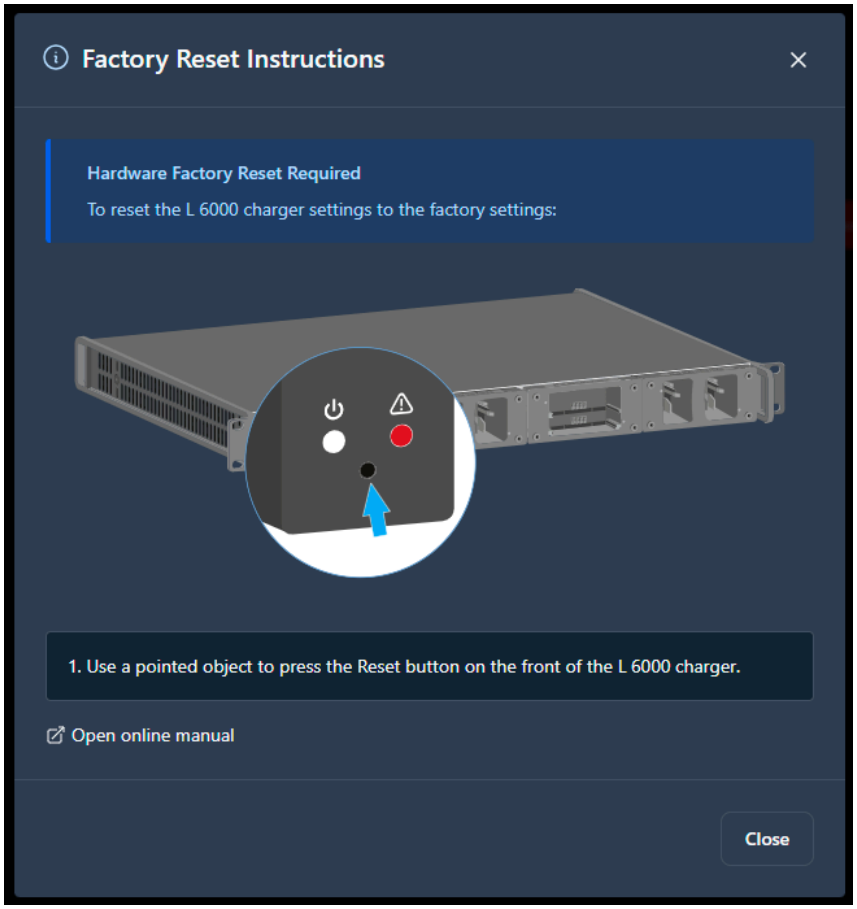
- Watch the progress indicator.
  - The device will reappear with default settings.

✓ The device has been set back to factory settings.

Resetting the L6000 charger

Reset the L6000 charger to factory settings.

L6000 chargers require a physical reset. Initiating a factory reset on an L6000 charger opens a modal with visual instructions for the physical reset procedure. The modal displays an image indicating the location of the Reset button on the front of the device, along with the instruction text. A link to the online manual is provided for additional context.



To reset the L6000 charger:

- Initiate the factory reset on the L6000 charger.
- Follow the visual instructions in the modal to perform the physical reset.
- Use the online manual link if you need more context.

✓ The L6000 charger has been successfully reset to factory settings.

Resolving security certificate warnings

Resolve blocked devices after a security certificate changes unexpectedly.

The Firmware Updater detects when a known device's security certificate changes unexpectedly, for example after a factory reset outside the application or because of a potential security threat.

- Affected devices appear in a blocked warning state with a red security alert indicator.
- A blocked device cannot be used in any workflow until you resolve the warning.
- A modal lets you accept the new certificate or remove the device from the list.
- Unresolved certificate conflicts are restored when you restart the application.
- Security alerts are fully localized in English, German, Spanish, and French.

> **i** You can resolve certificate alerts for multiple devices at once with bulk security certificate resolution. The selected action applies to all eligible devices. Devices without an alert in the selection are excluded automatically and remain unaffected.

To resolve the security warnings:

1. Under **Device Inventory**, click on **Resolve Security Alerts**.
   ✓ The security alerts are shown.
2. Choose one of the following options:
   - **Remove device** to remove the device from the list, or
   - **Accept new certificate** to accept the new certificate.

✓ The security certificate warnings have been resolved.

5. Knowledge base

Central hub for information, resources, and guides with further content on the product and/or service.

This page provides an overview of additional information such as instructions, know-how, best practices, and other links for the product.

Helpful links

- Firmware Updater

PDF downloads

Download	Document
	Admin Guide This guide provides IT professionals with a concise overview of the Sennheiser Firmware Updater for EW-DX devices.

FAQ

This section contains answers to frequently asked questions and further information.

If the devices are not discovered

When the devices are not appearing:

- Check that the devices are powered on.
- Ensure the devices are connected to the same network.
- Try refreshing the device list.
- Attempt to add the device manual by using the IP address, see Adding devices.

Check the network connectivity:

- Verify the network connections.
- Check the Firmware Updater and devices are on the same network subnet.
- Test device reachability with manual IP addition.

If the firmware update failed

The update failed:

- Check device connectivity before starting updates.
- Ensure devices are not busy with other operations.

- Verify stable network connection during updates.
- Look for specific error messages and suggested solutions.

A common error message appears:

- **Update failed due to network interruption**
  - Check the network and retry.
- **Device powered off during update**
  - Check the power source and restart the process.
- **Incompatible firmware file**
  - The firmware prevented the update from starting.

> **i** For offline updates, verify that the local firmware image matches the device model and version and that the file is not corrupted (checksum validation).

If a bulk operation partially failed

Some devices in the batch did not complete:

- Review the post-operation summary — successful and failed devices are listed individually
- Failed operations are automatically retried once before being flagged; retry the remaining failed devices independently
- Confirm that failed devices are online, reachable, and not busy with other operations
- Remember that ineligible devices are silently excluded from a bulk action and reported in the summary

If you have password and security issues

Changing the password failed:

- Verify the device is online and reachable.
- Check that the password complies with the complexity requirements.
- Ensure the device is not busy with other operations.
- Try again after a brief wait.

The device can not be claimed:

- Check the network connectivity to the device.
- Verify the device is powered on and responsive.
- Ensure the device hasn't already been claimed.
- Try refreshing the device list and attempting again.

A security certificate warning appears on a known device:

- This can occur after a factory reset performed outside the application, or may indicate a potential security threat
- Review the alert and either accept the new certificate or remove the device from the list
- The device remains blocked and unusable until the warning is resolved

If you are installing on macOS

The application will not install or launch:

- Confirm you are running macOS Ventura, Sonoma, or Sequoia on Apple Silicon (M-series); Intel Macs are not supported
- Install by dragging the application from the DMG into the Applications folder
- The application is code-signed and notarized, so no security warnings should appear — if the required .NET 8 runtime is missing, use the download link provided by the application

If you have performance issues

The response is slow:

- Use smaller page sizes for better performance.
- Apply filters to reduce the number of visible devices.
- Close other applications if experiencing slowdowns.
- Refresh the application if data seems outdated.

If you have large inventories:

- Use pagination effectively (recommended: 50 devices or less per page).
- Apply filters to focus on relevant devices.
- Use search to quickly locate specific equipment.

If you have interface issues

The display has problems:

- Try toggling dark mode on/off to refresh interface.
- Check that your browser supports the application.
- Clear browser cache if interface elements aren't loading properly.
- Ensure adequate screen resolution for an optimal display.

Other problems

This manual covers all functionality available in the 1.3.0 release. For additional support, please contact our technical support team or submit a request at at help.sennheiser.com/request.



Sennheiser electronic SE & Co. KG | Am Labor 1 | 30900 Wedemark | Germany