



Jabra Plus Management platform

Generated: July 16, 2026

Table of Contents

1	Introduction to Jabra Plus Management platform
1.1	Background
1.2	Before you begin
1.3	Customer security responsibilities
1.4	Compatibility and migration guide
1.5	Supported Jabra devices
1.6	Browser and security considerations
2	Quick Start Guide
2.1	Creating an account and choosing your interface langu...
2.2	Creating an organization
2.3	Enabling single sign-on
2.4	Inviting additional non-SSO admin users
2.5	End of QSG – Next Steps
3	Walkthrough: Suggested configuration
4	Managing the platform
4.1	Managing the platform
4.1.1	Dashboard
4.1.2	Organizations
4.1.3	Roles and permissions
4.2	Personal device management
4.3	Meeting room device management
4.4	JabraCLI - Offline device management

4.5 Integrating with other software

4.5.1 Integrating other software with Jabra Plus Management

5 Configurations

5.1 Configurations for Jabra personal devices

5.2 Room configurations for Jabra meeting room devices

5.3 Assigning a configuration to a device group or a room

5.4 Settings lock for Jabra device models

6 Firmware management

7 Software clients & Jabra Plus apps

7.1 Jabra personal devices – Jabra Plus Desktop software cl...

7.2 Jabra meeting room devices – Software clients

7.3 Deleting Jabra Plus clients

8 Appendix for Management Platform

8.1 Limitations

8.2 Device Management System matrix

8.3 Migrating from Jabra Xpress to Jabra Plus Management

8.4 Disabling data collection

8.5 Firmware bundles and specific firmware versions

8.6 Duplicating a configuration for personal or meeting ro...

8.7 Bulk-assigning a room configuration to many rooms

8.8 Rebooting Jabra meeting room devices

8.9 Pairing your Jabra personal devices to work with Jabra ...

8.10 Recovering your Jabra personal device after a failed fir...

8.11 Changing the Jabra Plus Management platform interfa...

9 Troubleshooting

1 Introduction to Jabra Plus Management platform

Jabra Plus is a cloud-based, comprehensive digital ecosystem designed for efficient remote management of Jabra devices, meeting business needs through interconnected digital touchpoints.

Jabra Plus starting point is the **Jabra Plus Management** platform – a multi-tenant Software-as-a-Service (SaaS) platform for IT administrators that centralizes management of Jabra meeting room devices, personal devices, speakerphones and other peripherals, offering features like usage tracking, advanced analytics, and real-time room availability, further providing a global oversight of meeting room device fleets and personal devices.

Jabra devices are provisioned to the platform via Jabra Plus software clients that are either built-into the device, must be downloaded from the platform or by using a companion app. After provisioning, Jabra devices can be remotely managed through the platform.

Every user of the platform is an **admin user** and is subdivided into *owners* and *members*, each with their own set of privileges enabling them to manage, monitor, and integrate devices remotely.

Using **locations** or **device groups**, you can group different Jabra meeting rooms or personal devices to sort virtual inventories as well as create and apply configurations to specific rooms or device groups.

The **Jabra Plus** ecosystem includes the following:

- **Access and Components**

There is client software connecting Jabra devices to the platform, automatically detecting and adding them to virtual inventories, i.e., **Jabra Plus Provisioning** (Provisioning app) and **Jabra Plus Desktop** (End user app).

- **Device Management**

Virtual inventories provide an overview of Jabra device models, enabling mass deployments, firmware updates, and settings management. You can group devices using **locations** or **device groups** to apply custom configurations. Standardized configurations ensure compliance with corporate policies and provide centralized access to advanced data insights.

- **Data Management**

Jabra Plus software clients collect and send device data, usage metrics, and user data to the platform. Real-time data tracking is enabled by default; however, data collection can be disabled for privacy reasons, or you can select specific data to collect.

The platform can be accessed at <https://cloud.jabra.com>

1.1 Background

The following are examples of features/services in Jabra Plus:

- **Cloud APIs**

A REST API that lets connecting systems perform several operations for a given organization, for example:

- Upgrade the firmware of individual Jabra personal and meeting room devices
- Get and/or set properties on Jabra personal or meeting room devices
- Collect telemetry data (such as metrics, logs, and analytics data) streaming from Jabra personal or meeting room devices

In addition to the API, integrations in Jabra Plus send events directly to a REST endpoint specified by the organization — this is referred to as webhooks. Also, the admin user in the relevant organization can specify which events must be sent via webhooks.

- **Jabra Plus Management platform**

An integral part of Jabra Plus enabling admin users to perform Jabra-device related tasks. All operations supported by the Cloud APIs can also be performed from the platform, for example:

- Administering a large number of Jabra personal and meeting room devices
- Specifying settings for different Jabra device types
- Event management
- Advanced meeting room management

The platform's web-based interface has features that help generate and administer components such as software clients, meeting room management, role management, as well as integration management to help set up integrations with third-party systems.

- **Offline device management**

Offline device management is possible via the JabraCLI tool – a command-line tool for Jabra devices that enables scripted, fully offline firmware updates, and offline configuration including changing device settings. See the JabraCLI – Offline device management section for details and guidance

1.2 Before you begin

This guide is intended for an admin user who would like to understand and use all the features of the **Jabra Plus Management** platform (the “platform”). It begins with a [Quick Start Guide](#) (QSG) that helps you create an account and an organization, enable single sign-on (SSO) and/or invite additional admin users.

After you complete the procedures in the QSG, you must provision Jabra personal and/or meeting room devices into the platform using the [Device Provisioning & Onboarding Guide](#). Device provisioning can be performed by you, the admin user, or it can be delegated to an external party or audio-video installer (AV Installer).

After provisioning Jabra devices, you can continue to the Suggested Configuration walkthrough to set up the **Jabra Plus Management** platform, as well as find reference information and procedures for remotely managing one or more Jabra devices.

In Jabra Plus documentation, “end users” refers to users whose Jabra personal devices are provisioned and managed in the **Jabra Plus Management** ecosystem. However, when the documentation refers to “end user computer” it refers to a computer/computing device connected to a Jabra personal device.

For further information, assistance, or feedback, contact [Jabra Support](#).

Limitations

Refer to the [Appendix](#) for information regarding any limitations of the **Jabra Plus Management** platform or Jabra devices within the platform.

1.3 Customer security responsibilities

Jabra is responsible for securing the **Jabra Plus Management** platform and the underlying cloud infrastructure it runs on.

On the other hand, your organization is responsible for securing your own environment and for how you use the platform. While not an exhaustive list, the following points describe areas where we rely on your organization’s own policies and processes.

Identity, access, and organization ownership

Your organization is responsible for:

- **Deciding** who acts as *organization owner* and ensuring this role is held only by trusted, authorized personnel, as owners can manage organization settings (device data collection), invite/remove admin users, change roles, and delete the organization
- **Assigning** appropriate roles (*owner, member with edit rights, member with read-only rights*) based on job responsibilities and [updating these roles](#) when responsibilities change
- **Removing** admin access promptly when staff leave or change role, including removing [non-SSO admin users](#) where applicable.

Use of single sign-on (SSO)

If you [enable SSO](#) with Microsoft® Entra, your organization retains responsibility for:

- **Managing** identity and access policies in Microsoft® Entra for users who access **Jabra Plus Management** (such as Multi-Factor Authentication, conditional access, and password policies)
- **Controlling** which users and groups are granted access to the platform and adjusting these assignments when staff join, move, or leave
- **Maintaining** the security of your Microsoft® Entra tenant and monitoring sign-in activity as part of your own security operations.

Browser, endpoint, and network environment

To ensure secure and reliable access to the platform, your organization is responsible for:

- **Installing** supported browsers on computers that access the platform, and keeping operating systems and browsers patched according to your internal policies
- **Applying** your standard endpoint security controls (for example, anti-malware and host-based firewall protection) to admin users' computers
- **Configuring** your network and security infrastructure (such as firewalls, proxies, VPNs, or secure web gateways) to allow outbound connectivity to the domains, subdomains, and ports required by the platform. See the list in the [Detailed whitelist domain requirements section](#).

Configuration, device management, and data handling

Within Jabra Plus Management, your organization controls how Jabra devices are managed. As an admin user, you are responsible for:

- **Establishing** internal standards for managing Jabra personal and meeting room devices, including how Jabra device settings, configurations, and firmware updates are applied
- **Ensuring** that only *owners* and *members with edit rights* perform critical actions. For details, see the [roles and permissions matrix](#)
- **Handling** any exports (for example, exporting the device inventory table or list) in line with your own security, privacy, and retention policies
- **Informing** your end users about how Jabra Plus Management is used to manage Jabra devices, based on your legal and privacy obligations.

Monitoring, activity review, and incident handling

Your organization is responsible for:

- **Viewing** admin user activity or history and integrating relevant activity information (for example, activity logs – device details and meeting room activity) into your broader monitoring and audit processes where needed
- **Training** all admin users/AV Installers to recognize and report unusual or unauthorized activity
- **Following** your internal incident response procedures if you suspect unauthorized access, account compromise, or misconfiguration related to Jabra Plus Management, contact [Jabra Support](#) for further assistance.

Jabra Plus Security Framework Guide

- For a complete overview of the suggested security considerations, including technical information about data storage, architectural overview, and others, you can request the Jabra Plus Security Framework Guide from a Jabra representative.

1.4 Compatibility and migration guide

The platform is compatible with an array of Jabra hardware such as meeting room devices (including extension devices such as a Jabra scheduler) and personal devices (including Jabra speakerphones). In certain cases, you can also use the platform alongside other device management systems.

Be aware that using other Jabra software, such as **Jabra Xpress** or **Jabra Direct**, together with **Jabra Plus** may inadvertently cause potential conflicts with Jabra hardware.

If you are migrating from **Jabra Xpress**, see the [Migrating from Jabra Xpress to Jabra Plus Management](#) topic.

Compatibility with other device management systems

See the [Device Management System matrix](#) in the appendix, informing you of potential known issues and offering recommendations when more than one device management system is used at the same time with the platform.

1.5 Supported Jabra devices

The list of supported Jabra devices is routinely updated and can be found on the following [link](#).

Important note

Certain older Jabra devices' firmware cannot be updated via the **Jabra Plus Management** platform. Instead, they must be updated using **Jabra Direct** or **Jabra Xpress**.

You can still use the older Jabra devices on the platform and change settings, however, depending on the firmware version you are running, the list of settings that you can modify can also change.

To find out whether your device can be firmware updated or not, see the [list of supported Jabra devices](#).

1.6 Browser and security considerations

To log in to the platform, as a prerequisite, the computer must have the latest versions of the following browsers installed:

- Google Chrome™
- Microsoft® Edge

Security considerations

For the platform to work as intended, it is recommended that certain outbound TCP ports are open. See the [Appendix](#) for the domains, subdomains, and outbound ports that must be accessible to the platform.

Code signing

All **Jabra Plus** software clients are digitally signed Microsoft Software Installer (*.msi) files, adhering to Microsoft's best practices for enhanced file security, authenticity and code integrity.

When launched, the Installer unpacks dependencies, including digitally signed Dynamic Link Libraries (.dll) and executable (*.exe) files.

When dependencies are unpacked, certain file extensions i.e.: ***.json**, ***.temp**, ***.version**, ***.xml**, and ***.config** are not digitally signed, as they do not present a risk to overall security.

2 Quick Start Guide

All procedures in this chapter are mandatory unless stated otherwise.

Step 1

To quickly get started with the platform, you must perform both procedures in the following order:

a. Creating a Jabra Plus account

b. Creating an organization

After creating an account, you must log in and you are prompted to create an organization (such as a business or corporation), which is a representation of the company/business on the platform.

When creating an organization, data tracking and data collection are enabled by default. Although you can [disable data collection](#) at a later time, it is recommended that you review and decide on the data collection settings before provisioning Jabra devices to the platform.

After creating the organization, you become the *owner* (of the organization) and can then choose how to grant access to subsequent admin users. This is done by either enabling single sign-on (SSO) and using Microsoft® Entra for user management or you, the *owner*, can manually invite additional admin users to the platform.

Note

After creating the organization, the admin user's (*owner*) account cannot be deleted. This is because there must always be one admin user that has access to the organization, i.e.: an admin user that can manually log in using their email address.

Step 2 (Optional)

After creating an account and an organization, you can enable SSO and invite additional admin users to the platform. Both of the following procedures are optional. If you do not wish to do so, you may continue to [End of QSG – Next steps](#).

a. Enabling single sign-on (SSO)

b. Inviting additional admin users

Only *owners* and *members with edit rights* in the **Jabra Plus Management** platform can download organization-specific software clients, manage Jabra devices remotely, set the settings for one or a group of Jabra devices, manage the firmware, and more. For conceptual information on the different components of the platform, read the [managing the platform](#) chapter.

2.1 Creating an account and choosing your interface language

In the **Jabra Plus Management** platform, you must first create a **Jabra Plus** account and choose the interface language.

Note

When creating a **Jabra Plus** account, the default interface language is initially based on your browser settings.

Choosing an interface language on the platform only applies to your **Jabra Plus** account. Subsequent admin users can change their own interface language when they initially log in, or they can change the interface language following the [changing the Jabra Plus Management platform interface language](#) procedure in the appendix.

To create an account and choose the interface language:

1. In a web browser, enter the following URL: <https://cloud.jabra.com>
2. In the **Log in to Jabra Plus Management** pane, click **Create account**
3. On the **Jabra Login** page, click **Sign up now**
4. On the **Create Account** page, enter your business email address, and click **Send verification code**
5. At this point, you receive a confirmation email with a verification code. Ensure you copy the verification code, and then return to <https://cloud.jabra.com>
6. On the **Create Account** page, ensure you enter the code, click **Verify code** and then click **Continue** on the next screen
7. On the **Create Account** page, you must choose your **Country / Region** and on the *Display name* field you must enter a name or alias, as this is your username on the platform. Ensure you also create a password following the guidelines, accept the **Terms of Service** and then click **Next**
8. Once you log in to the platform, in the **Welcome to Jabra Plus Management** dialog, in the **Language preference for personal account** drop-down menu, choose your language and click **Create organization**

After your initial sign-in to the platform, the *owner* is prompted to create an organization.

2.2 Creating an organization

After you complete the sign-up (first-time registration) process for an account and log in to the platform with your email domain, you, the admin user (now the *owner*), are prompted to create an organization, for example, *ABC Company*.

For conceptual information and guidance, see the [Organizations](#) topic.

To create an organization upon first-time login:

1. In the **Create organization** dialog, in the **Name** field, enter a name for your organization. Ensure you provide a meaningful name, as there may be a need to invite additional admin users to the organization

Note

The platform supports ASCII and non-ASCII characters, such as accented letters, non-Latin alphabets, and symbols, however an organization cannot be renamed, so ensure the naming of the organization is correct.

2. In the **Type** dropdown menu, select the level of access and click **Continue**
3. In the **Welcome** dialog, ensure you read the license agreement and privacy policy and then click **Accept**
4. In the **Choose device information to collect** dialog, check the relevant checkboxes, and to save your selections, click **Continue**. For more information about data collected, see the [disabling data collection](#) topic in the appendix
5. In the **Organization created** dialog, click **Get started**. You are now the *owner* of the organization you created and are directed to the [Dashboard](#)

At this point, you can enable SSO to grant additional admin users' access to the organization. Otherwise, if SSO is disabled, you can follow the [inviting additional admin users](#) procedure.

2.3 Enabling single sign-on

An organization *owner* can enable SSO to access the platform. This ensures that only admin users from pre-approved domain(s) can log in and access the organization.

Note

If you have multiple organizations under the old SSO, you can only associate the new setup with one organization. For more details, request the **SSO Optional Migration Guide** from your Jabra representative.

When SSO is enabled, all admin users authenticate their access to the platform using Microsoft® Entra and can only access the one organization. By default, all admin users are given *read-only* access. Further access rights i.e. granting *owner* or *edit* permissions for meeting rooms and/or personal devices is assigned exclusively within Microsoft® Entra.

For guidance, see the [Roles and permissions](#) topic.

When SSO is enabled, certain functionalities are not available on the platform, for example, admin users cannot edit permissions, change their **Jabra Plus** profile or leave an organization.

If the organization does *not* want to use SSO for access, an *owner* can [invite other admin users](#) manually. If needed, you can also disable SSO and after two hours, admin users can no longer log in to the organization using SSO.

To enable SSO for all admin users in the organization:

1. In a web browser, enter the following URL: <https://cloud.jabra.com>
2. In the **Log in to Jabra Plus Management** pane, in the **Email** field, enter your business email address and click **Continue with email**
3. On the left-hand navigation bar, at the bottom of the page, click the name of the organization you are currently the *owner* of, and then click **Organization settings**
4. On the **Organization settings** page, in the **Enable single sign-on (SSO)** pane, click **Enable**
5. In the **Sign in to SSO provider** dialog, click **Sign in**

At this point, you are prompted to sign in to Microsoft® Entra, and then verify and accept the permissions requested.

Important note

- **Admin mode:** To enable Microsoft Entra ID to be used with the platform – on Step 5 of this procedure – you must log in to Microsoft® Entra with a Microsoft Entra ID admin user account holding the [Application Administrator](#) role, and you must also check the *Consent on behalf of your organization* checkbox, allowing all users in your organization to get access to the relevant resources. Doing so creates the **Enterprise Application** in Microsoft® Entra, granting consent to **Jabra Plus Management** and letting you assign and manage user access to enterprise applications.
- **Non-admin users requesting consent:** If you are *not* a Microsoft Entra ID admin user, you must request consent from one. However, to do this, the **Admin consent requests** option in Microsoft Entra ID [must be enabled](#). When the non-admin is granted consent by the relevant Microsoft Entra ID admin user in your business organization, you must sign in again to enable SSO.

6. In the **Jabra Plus Management** platform, in the **Single sign-on enabled** dialog, click **OK**

To continue, return to Microsoft® Entra and grant additional admin users' access to the platform. For details on the scope of roles, refer to the [Roles and permissions](#) chapter.

After enabling SSO and granting access to other users, the admin user can continue with the [End of QSG – Next Steps](#).

2.4 Inviting additional non-SSO admin users

If SSO is disabled, an *owner* can invite other admin users (i.e.: additional *owner* roles and/or *members* with either *edit rights* or *read only rights*) manually to grant them access to an organization. Admin users who were invited via email (users who must log in to Jabra Plus Management using their email and password they created) to the organization are **non-SSO** users.

For guidance regarding roles and permissions, see the [Roles and permissions](#) topic.

Adding a second *owner* to an organization is recommended, as it can be helpful if access to the platform is lost. Only an *owner* can invite a new admin user, send, resend or revoke invitations, and edit permissions on behalf of all admin users in the organization.

After manually inviting additional admin users (when SSO is disabled), user management for non-SSO users takes place exclusively within the **Jabra Plus Management** platform. For procedures, refer to the [Changing roles and editing permissions of non-SSO users](#) and [Removing a non-SSO user](#) topics.

An *owner* can invite one or multiple admin users, and invitations are valid for seven days.

To invite one or more non-SSO admin users to the organization:

1. On the bottom left-hand side of the navigation bar, click the name of the organization you are currently the *owner* of, and then click **Admin users**
2. On the **Admin users** page, on the top right-hand side of the screen, click **Invite new user**
3. In the **Invite new user** dialog, in the **Email** field, enter the new admin user's business email address
 - To invite multiple *members* with the same permissions or additional *owners*, separate the email addresses with a comma (,) or semicolon (;)
4. In the **Role** section, click the relevant radio button for **Member** or **Owner**
 - When selecting the *Member* role, in the **Permissions** section, for **Meeting rooms** and/or **Personal devices** management, click **Edit** or **Read only**
5. Click **Invite**

At this point, **Jabra Plus Management** sends an email prompting the recipient to create a **Jabra Plus** account using a unique sign-up link. After creating an account, the added admin user can log in to the platform.

2.5 End of QSG – Next Steps

You are now the *owner* of an organization, and you may or may not have invited additional admin users to the platform.

The next step is to provision Jabra devices to the newly created organization. For procedures you can refer to the [Device Provisioning & Onboarding Guide](#).

When you have finished provisioning Jabra devices to the platform, you can continue to the [Suggested configuration of the Jabra Plus Management platform](#) topic to begin configuring it.

Device provisioning methods and strategies

To add Jabra devices to the platform – and depending on your type of Jabra device, the admin user can perform the software client installation, generate an *organization provisioning code/room provisioning code* and/or download the **Jabra Plus Provisioning** app.

You can also delegate the provisioning to an AV Installer or third-party. For example, depending on the Jabra device, an admin user with the relevant permissions must provide the third-party with the software client(s) and/or the desired provisioning code type.

If you would like to provision Jabra meeting room devices to the platform, or delegate provisioning to an AV Installer, you must decide on the strategy:

- *Organization provisioning code* lets you add the device to the platform and to your organization to an empty location first and then add a configuration and/or a firmware policy manually. This approach works if you want to focus on provisioning all devices first and you do not have a Locations/Room structure in place.
- *Room provisioning code* can be used when you create a Locations/Room structure first which can include a configuration and/or firmware policy, and you then provision Jabra device(s) directly to that specific room. See the [Provisioning Codes](#) topic for guidance and procedures.

The following table outlines the types of Jabra devices and their respective provisioning method.

Type of Jabra device	Required provisioning method	Pre-requisite step performed by an admin user
Jabra personal devices (e.g. Evolve3 85, Engage 50, etc.) ¹ Note: Includes Jabra speakerphones (e.g., Speak2 75, etc.)	Jabra Plus Desktop app ²	Create and download Jabra Plus Desktop
Jabra meeting room device Jabra PanaCast 50 Room System (RS) ³	Room client ²	Create and download a room client
Jabra meeting room device Jabra PanaCast U30 or Jabra PanaCast 40/50/55 Video Bar System (VBS)	An <i>Organization</i> or <i>Room provisioning</i> code	Viewing or generating a room or organization provisioning code
Jabra meeting room device Jabra PanaCast 50 — Bring Your Own Device (BYOD)	Jabra Plus Provisioning app and an <i>Organization</i> or <i>Room provisioning</i> code	Download Jabra Plus Provisioning and Viewing or generating a room or organization provisioning code

- ¹ Includes Jabra speakerphones (e.g.: Speak2 75, etc.).
- ² **Mass deployment option:** An admin user or AV Installer can perform the software client installation in a mass deployment context. For guidance, see **Mass deployment** in the [Software client installation & device provisioning](#) topic in the Jabra Plus Device Provisioning & Onboarding Guide.
- ³ Includes any certified Microsoft Teams Rooms (MTR) or Zoom Rooms (ZR) meeting room computer (Windows PC with a screen/interface) that is permanently connected to the Jabra PanaCast 50.

3 Walkthrough: Suggested configuration

At this point, you may have completed the QSG and provisioned Jabra personal or meeting room devices. Admin users with the appropriate [permissions](#) can now configure the platform.

When Jabra devices are provisioned, they are added to the **device inventory** or **room inventory** and are automatically assigned a default **standard configuration**, which is a collection of Jabra-recommended settings that include a default firmware policy.

Admin users can begin remote management with Jabra's default configuration or optionally customize it to suit the organization's needs.

If an admin user manages a few Jabra personal or meeting room devices, they can [adjust settings remotely of a single Jabra meeting room device](#) or [adjust settings remotely of a single Jabra personal device](#), without using a predetermined configuration and/or without having the Jabra device within a grouping (such as **locations**).

However, if you manage many Jabra devices, it is recommended that you follow the subsequent configuration procedures:

For Jabra personal devices

- [Pair your Bluetooth Jabra personal devices to the USB dongle \(Jabra Link Bluetooth adapter\)](#)
- [Create device group\(s\) and sort Jabra personal devices](#)

For Jabra meeting room devices

There are two ways to provision Jabra meeting room devices into the platform based on your chosen strategy:

- **Provisioning devices**

Use the [organization provisioning code](#) to add devices (with built-in clients) as *unassigned rooms* to the room inventory. Name devices during provisioning, then later assign room configurations/firmware policies.

Note

The Jabra meeting room device that requires a room client for provisioning i.e.: Jabra PanaCast 50 Room System, always appears as an *unassigned room* after provisioning, and can be manually moved into a location.

For guidance, read the *Device provisioning methods* section in the [End of QSG – Next Steps](#) topic.

- **Creating a room structure**

Add a room (empty) to create a room structure (optionally you can assign a room configuration and/or firmware policy to the room) and then use a room provisioning code to provision a meeting room device directly into the added room.

For either of the strategies, you can optionally complete the following:

- Add a locations structure based on how the business organization is organized
 - Move your unassigned or empty rooms into locations and add details to rooms
- Define a schedule for Jabra meeting room device firmware updates

Other optional tasks you can complete for *both* personal and meeting room devices:

- Configurations: use **standard configuration** with or without exceptions (For Personal or Meeting room devices) or create one i.e.: Create a configuration / Create a room configuration
 - Assigning a configuration or Bulk assigning a previously created **room configuration** to many rooms
- Firmware: You can customize firmware policies in configurations to suit your needs
 - Enable or disable firmware management
 - Choose whether you want to Modify & set the firmware policy for specific Jabra device models
 - Choose a specific firmware version for your Jabra devices to use, and others.

For reference information and to understand all the capabilities of the platform, see the [Managing the platform](#) chapter.

4 Managing the platform

4.1 Managing the platform

The **Jabra Plus Management** platform offers a web interface for managing Jabra personal and meeting room devices remotely. This chapter is a general reference for understanding the capabilities of the platform.

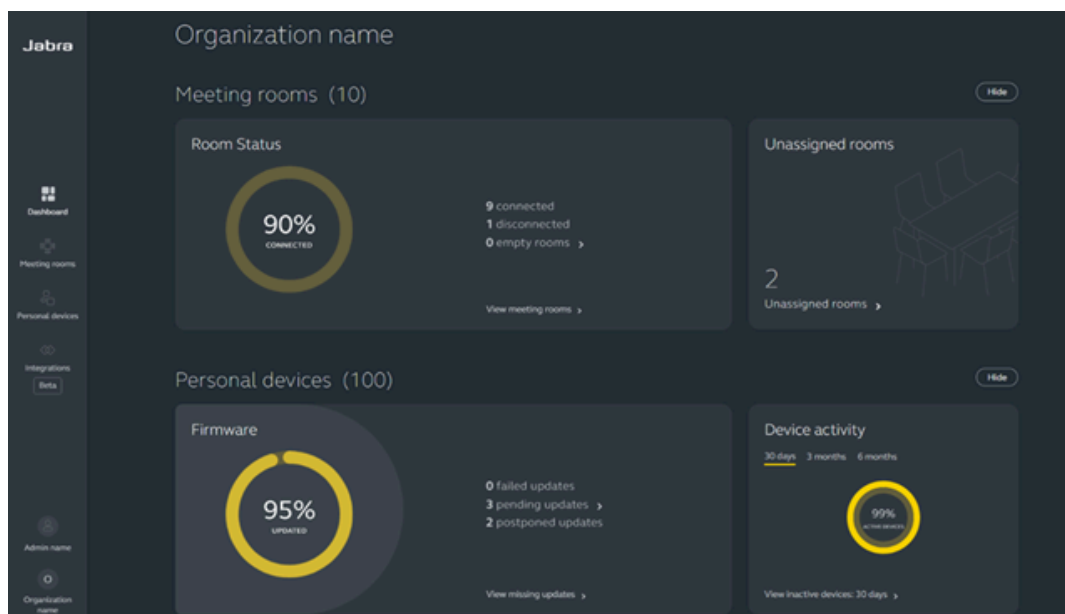
It is divided into platform management, [personal device management](#), and [meeting room device management](#). You can track assets, usage, access analytics, and perform mass firmware updates. Organizations such as a business, corporation, or subsidiary — are grouped under unique names, and devices are automatically added to inventories upon software client deployment.

You can customize configurations for specific Jabra personal and meeting room device models and view key metrics on the **Dashboard**, including Jabra device counts and activity.

4.1.1 Dashboard

The **Dashboard** provides an overview of the key Jabra meeting room and personal device information, including the total number of managed Jabra meeting room and personal devices in each organization, Jabra device activity, room status, firmware status, and other variables.

You can access the dashboard from the main page after logging into the platform or click the **Dashboard** menu on the left-hand navigation bar.



4.1.2 Organizations

An organization is a representation of your company/business on the platform with a unique organization ID. When you log in to the platform for the first time, you are prompted to create your organization, in which you take up the *owner* role.

Important note

When single sign-on (SSO) is enabled, admin users cannot leave an organization, invite other admin users, or modify their **Jabra Plus** profile.

Be aware that granting access or changing access rights for admin users is performed exclusively in Microsoft® Entra, instead of within the **Jabra Plus Management** platform. For details, see the [Roles and permissions](#) chapter.

Despite SSO being enabled, there must always be one admin user with access to the organization i.e.: manually logging in with their email address.

When SSO is disabled

When your organization is not using SSO, *owners* can manually invite other admin users (additional *owners* or *members*), and set their respective permissions i.e. *edit rights* or *read only* access for **Meeting rooms** or **Personal devices** within the **Jabra Plus Management** platform.

When SSO is disabled, a *member* can leave an organization independently; however, an *owner* can only leave an organization if they first [elevate](#) another user to the *owner* role.

Whether SSO is enabled or not, any *owner* can delete an organization altogether.

Deleting an organization

When an *owner* deletes an organization, it permanently removes all Jabra device data within the platform, and all Jabra devices in the **device inventory** and **room inventory** gradually stop sending device data.

Moreover, the connection to the platform that the relevant software client initially established is severed. However, the software client remains installed on end user computers or meeting room computers/computing devices until it is uninstalled from the devices on which it was installed.

Important note

Be aware that when an *owner* deletes an organization, Jabra personal and meeting room devices continue to operate, but the remote management of those devices within the platform is terminated.

The deletion process is not instantaneous and may take up to 24 hours to complete. All associated device data, usage data, and user data are then irrevocably deleted.

To delete an organization:

1. On the bottom left-hand side of the navigation bar, click the name of the organization you currently belong to, and then click **Manage my organizations**
2. Within the **Organization** pane of the organization you would like to delete, click the action menu (three-dot menu) and click **Delete organization**
 - a. If you do not see the **Delete organization** option, ensure you first click the action menu and then select the organization by clicking **Select organization** and then continue with the next step
3. In the **Delete organization** dialog, to confirm the deletion, click **Yes, continue**
4. In the **Delete organization** warning, check the **I confirm I want to delete the organization** checkbox, and click **Yes, delete organization**

After deleting an organization, the logged in admin user is prompted to create a new one. If there are other organizations created **Jabra Plus Management** makes the last active organization active.

Leaving an organization as a member

When SSO is enabled, *members* cannot leave an organization independently. This can only be done through Microsoft® Entra. Otherwise, when SSO is disabled and the *member* was manually invited to the organization, they can leave an organization on their own. For guidance, see the [Roles and permissions](#) topic.

To leave an organization as a *member* (non-SSO user):

1. The *member* who wants to leave the organization must log in to the platform using their email address
2. On the left-hand navigation bar, click the name of the organization you belong to, and then click **Manage my organizations**
3. Within the **Organization** pane (of the organization you want to leave), click the action menu and click **Leave organization**

4. In the **Leave organization** dialog, click **Leave** to confirm

At this point, the *owner* of the organization receives an email informing them that a *member* has left the organization.

Leaving an organization as an owner

When SSO is enabled, *owners* cannot leave organizations independently. Instead, this can only be done through Microsoft® Entra.

However, if SSO access is disabled, the admin user holding the *owner* role can leave an organization on their own provided that the organization has more than one admin user with the *owner* role, i.e.: an admin user that has access to the **Jabra Plus Management** platform using their email address.

In this case, the *owner* must first upgrade an admin user from *member* to *owner* in the **Jabra Plus Management** platform. For guidance, see the [Roles and permissions](#) topic.

After the *owner* has elevated an admin user from *member* to *owner*, the *owner* can leave an organization as follows:

1. The *owner* who wants to leave the organization must log in to the platform using their email address
2. On the left-hand navigation bar, click the name of the organization you belong to, and then click **Admin users**
3. On the **Admin users** page, on the list, find the row with your name and click the action menu (three-dot menu)
4. Click **Leave organization**, and in the **Leave organization** dialog box, click **Leave**

At this point, the new *owner* of the organization receives an email informing them that another *owner* has left the organization.

4.1.3 Roles and permissions

In **Jabra Plus Management**, roles and permissions depend on whether SSO access is enabled or disabled. For details about SSO setup, see the [Enabling single sign-on](#) chapter.

SSO vs non-SSO

- When SSO access is enabled: admin users (*owners* and *members*) cannot change admin roles, edit permissions, or remove admin users inside **Jabra Plus Management**. Those actions must be done in Microsoft® Entra.
- When SSO access is disabled (non-SSO): an *owner* can manage admin users from **Jabra Plus Management** — invite users individually, revoke invitations,

change roles, and terminate or remove member access.

Be aware that there is always at least one non-SSO admin user shown in the admin users list.

Organization ownership

The admin user who creates an organization becomes its *owner*. Admin users are system/IT administrators for Jabra devices in the organization and have one of two roles: *owner* or *member*. The roles are broken down as follows:

- **Owner**

- Elevated admin user with full administrative rights for the organization and all Jabra devices
- Can perform Jabra device provisioning, enable SSO, manage roles and permissions, and delete organizations
- Can change a member's role to grant access to managing meeting room devices, personal devices, or both
- Can promote a member to owner, downgrade other *owner(s)* to *member(s)*, or downgrade their own role — provided the organization retains at least one owner
- Can remove or terminate a member's access; exact ability depends on whether the user is an SSO or non-SSO user
- All admin users (*owners* and *members*) receive email notifications for any role or permission-scope changes

Be aware that when SSO is enabled, *owner* appears in Microsoft® Entra as *Jabra+ Organization Owner*.

- **Member**

- Subordinate to owners; cannot perform user-management tasks or change organization settings (for example, disabling data collection)
- Cannot change their own role. Non-SSO *members* can independently leave an organization
- Member types:
 - *Member with Edit Rights*: can manage and provision Jabra meeting room and/or personal devices according to assigned permissions
 - *Member with Read-Only Rights*: can view meeting room and personal devices and associated data but has no device- or user-management capabilities. When SSO is enabled, read-only is the default role assigned in Microsoft® Entra.

Be aware that a *member with edit rights* for one device category (meeting rooms or personal devices) has read-only access to the other, and *members* also cannot change organization settings, such as [disabling data collection](#). Finally, when SSO is enabled, a *member with edit rights* appears in Microsoft® Entra as *Jabra+ Personal Device Editor* and/or *Jabra+ Meeting Room Editor*.

Location-based access control for meeting rooms

Location-based access control lets organization *owners* control which locations an admin user can access in the **room inventory**.

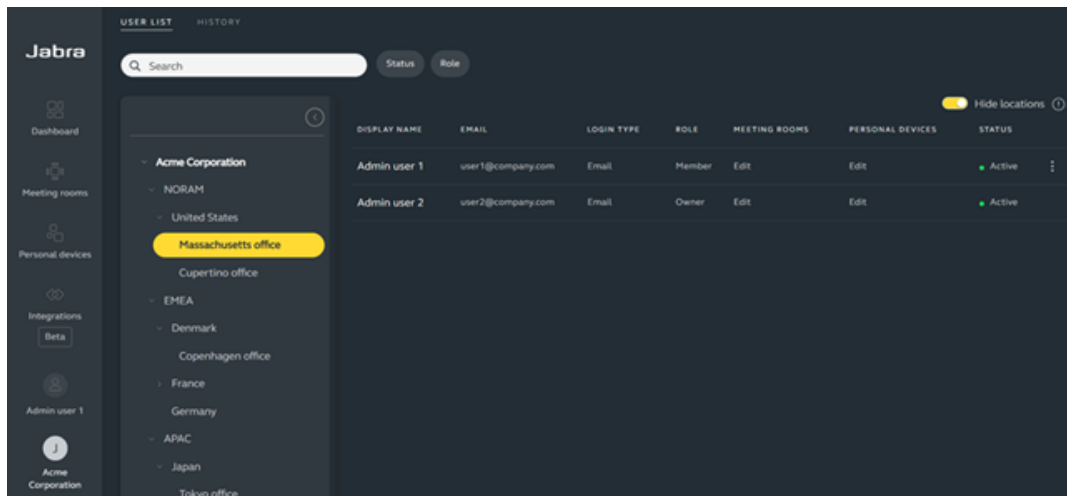
Organization *owners* can remove an admin user's **room inventory** access or limit the admin user's access to specific locations in the hierarchy. Access can be limited to a single location or to a parent location. When access is limited to a parent location, the user can also access all locations below it. The following example shows a location hierarchy:

- NORAM (*parent*)
 - United States (*child*)
 - Lowell office (*child*)
 - Cupertino office (*child*)

In the example above, if a user's access is limited to Cupertino office, the user can access only the **room inventory** for Cupertino office. The user cannot access the room inventory for NORAM, United States, or Lowell office. If a user's access includes NORAM (*parent*), the user can access NORAM and all locations below it, including United States, Lowell office, and Cupertino office.

Note

To show all available locations in the user list, switch off the **Hide locations** toggle on the top right-hand side of the user list.



Restricting access to meeting room locations and room inventory

To restrict an admin user's access to meeting room locations:

1. Log in to **Jabra Plus Management** with an account that has the *owner* role
2. On the left-hand navigation bar, click the name of your organization, and then click **Admin users**
3. On the **User List** tab, find the user whose location access you want to change. On the right-hand side, click the action menu (three-dot menu) and then click **Edit location permissions**
4. In the **Edit location permissions** dialog, check the location name's checkbox that you want to restrict this user from accessing, and then click **Save**

At this point, the admin user's permission scope is now restricted to the selected location(s).

Roles and permissions matrix

The following matrix shows interactions that an *owner* or *member* can or cannot perform within **Jabra Plus Management**.

Interactions	Owner	Member (edit rights)	Member (read only)
- Delete an organization - Change organization settings (data collection)	Yes ¹	No	No
- Invite new admin users to the organization - Change roles from <i>owner</i> to <i>member</i> (or vice versa) - Change permissions for <i>members with edit rights</i> to <i>read-only rights</i> (or vice versa) - Remove admin users (<i>owners</i> or <i>members</i>) from the organization	Yes ¹	No	No
- Leave an organization ¹	No ²	Yes	Yes
- View history (admin user activity log)	Yes	No	No
- Access the Meeting rooms menu item to view Jabra meeting room devices in the room inventory and associated data e.g.: created room clients, created room configurations, etc.	Yes	Yes	Yes
- Add a (empty) room - Name meeting rooms - Change Jabra meeting room device settings - Download Jabra Plus room clients - Create room configurations	Yes	Yes ³	No
- Access the Personal devices menu item to view personal device details, device inventory, device groups, installed instances of Desktop clients (Jabra Plus Desktop), number of Jabra devices provisioned, and Configurations menu items	Yes	Yes	Yes
- Add personal devices to the device inventory - Export the list of Jabra personal devices - Create device groups to sort Jabra personal devices - Create and assign configurations	Yes	Yes ⁴	No
- Enable or disable firmware management - Change firmware policies for an organization's Jabra devices	Yes	Yes ^{3,4}	No

Interactions	Owner	Member (<i>edit rights</i>)	Member (<i>read only</i>)
- Lock specific Jabra device settings and prevent end users from changing them	Yes	Yes	No
- Create and download software clients	Yes	Yes ^{3,4}	No
- Reboot Jabra meeting room devices	Yes	Yes ³	No
- Access the Integrations menu to grant or revoke access to the Jabra API portal and specify webhook endpoints	Yes	No	No

¹ When SSO is enabled, these actions are performed in Microsoft® Entra or not at all. Refer to the [Enabling SSO procedure](#).

² An owner can only leave an organization if there is another owner in the organization. Refer to the [Leaving an organization as an owner procedure](#).

³ Provided that the *member with edit rights* has been given access to Meeting room management. See the [Changing roles and editing permissions of non-SSO users](#) for the procedure.

⁴ Provided that the *member with edit rights* has been given access to Personal device management. See the [Changing roles and editing permissions of non-SSO users](#) for details.

Changing roles and editing permissions of non-SSO users

Important note

When single sign-on (SSO) is enabled, admin users cannot leave an organization, invite other admin users or modify their **Jabra Plus** profile.

Be aware that granting access or changing access rights for admin users is performed exclusively in Microsoft® Entra, instead of within the **Jabra Plus Management** platform. For details, see the [Roles and Permissions](#) chapter.

To change roles, edit permissions for non-SSO users:

1. Log in to **Jabra Plus Management** using your email address and *owner* role
2. On the left-hand navigation bar, click the name of the organization you are currently the *owner* of, and then click **Admin users**

3. On the **Admin users** page, on the list, find the user that you want to manage access rights for or to remove, click the action menu (three-dot menu) and click **Edit permissions**
 - a. To change the role of a *member* to *owner* or vice-versa, in the **Edit permissions** dialog, in the **Role** pane, select **Member** or **Owner**, and then click **Save**
 - b. To edit the access rights or permissions for a *member*, in the **Permissions** pane, select **Edit** or **Read only** for meeting rooms/personal devices, and click **Save**

For changes to apply, after changing the role of a user, the user must log out and log back in to the platform.

Removing a non-SSO user

To remove an SSO admin user from **Jabra Plus Management**, you must first remove the user from Microsoft® Entra and then perform the procedure that follows, in the platform.

This requirement is not necessary for non-SSO admin users, and it is due to user management in Microsoft® Entra not being synced with **Jabra Plus Management**.

For procedures on how to remove a user from Microsoft® Entra, refer to Microsoft documentation.

To remove a non-SSO admin user:

1. Log in to **Jabra Plus Management** using your email address and *owner* role
2. On the left-hand navigation bar, click the name of the organization you are currently the *owner* of and then click **Admin users**
3. On the **Admin users** page, on the list, find the user that you want to terminate access for, and click the action menu
4. Click **Remove admin user**, and in the **Remove admin user** dialog, click **Remove**

If the removed *member* was also an admin user in other organizations, the removed user maintains their membership in the other organization(s); however, the removed member can also be reinvited.

Viewing admin user activity or history

To enhance security and accountability, the platform logs admin user activity to monitor, track, and manage user activities in an organization.

On the platform, the **History** tab in the **Admin users** menu keeps a log of any changes to access rights, user invitations, and access terminations for 30 days.

The admin user with the *owner* role can view admin user activity or history on a filterable list. The list contains details such as *Time*, *Impacted Entity*, *Event*, and *User*.

To view admin user activity:

1. On the left-hand navigation bar, click the name of the organization you are currently the owner of, and then click **Admin users**
2. On the **Admin users** page, click the **History** tab

The history of admin user activity in the organization is now visible on a list that can be sorted by *Time*, *Impacted Entity*, *Event*, and *User*.

4.2 Personal device management

In the **Jabra Plus Management** platform, the **Personal devices** menu item lets you visualize, sort, and configure Jabra personal devices to effectively manage them in an organization.

Personal devices are audio devices such as headphones, headsets and speakerphones; Personal device management addresses the challenges of remote identification, management, and troubleshooting of Jabra personal devices.

In a managed context, the **Jabra Plus Desktop** app lets you, the admin user, perform bulk management of settings and firmware, inspect real-time Jabra personal device status, remotely adjust settings on behalf of end users, and other functionalities via the **Jabra Plus Management** platform.

Like meeting room devices, Jabra personal devices have a virtual inventory, or **device inventory**. The **Personal devices** menu item is made up of the [Device inventory for personal devices](#), [Configurations](#), [Device groups](#), and [Desktop clients](#).

Device groups act as the foundation to assign configurations, and custom firmware policies that takes effect on specific groups of Jabra personal devices.

This grouping mechanism is designed to give you an overview of all your Jabra personal devices, and help you group or classify the devices based on real or made-up variables, such as countries, cities, building or department names, etc.

To provision personal devices, you must install **Jabra Plus Desktop** on all end user computers. After provisioning, Jabra personal devices appear in the **device inventory** and you can then [adjust settings remotely](#) of a single Jabra personal

device and/or to Create device groups and sort Jabra devices into Device groups.

For guidance, see the [Walkthrough: Suggested configuration of Jabra Plus Management platform](#) chapter.

Device inventory for personal devices

The **device inventory** is a repository for all Jabra personal devices (including speakerphones) added to an organization. It is automatically populated when the **Jabra Plus Desktop** app is deployed and installed on your end user's computers and end user Jabra personal devices are [paired](#) (Bluetooth Jabra devices) or recognized by the app automatically (cabled or wired Jabra devices).

In a searchable and filterable list, the **device inventory** outlines information such as *Device model*, *Connection status*, *Firmware status*, any *Device group(s)* it may belong to, (device) *Serial number*, *Firmware version*, *Username*, *Computer name*, *Client name*, *Client version*, *Last seen*. In the **device inventory**, the collected device data lets you search for keywords such as *Computer Name* or *Windows Username*.

Note

When a device serial number is not available, cannot be displayed or cannot be fetched from the device, be aware it is replaced by the **Electronic serial number**.

For more information about device data collection, see the [Disabling data collection](#) topic in the appendix.

In addition, you can further sort Jabra personal devices in the **device inventory** into **device groups**, effectively creating a secondary grouping in the organization.

For example, an admin user may want to group Jabra devices in the organization into different departments, such as Marketing, Human Resources, etc. You may also want to classify Jabra personal devices in device groups based on the location of Jabra devices or another useful variable.

When Jabra personal devices are added to the **device inventory**, a default standard configuration is applied to all Jabra personal devices in the inventory. You can also manually remove Jabra personal devices from the **device inventory**.

Adding Jabra personal devices to the device inventory

For procedures, see the [Device Provisioning & Onboarding Guide](#).

Removing Jabra personal devices from the device inventory

You can also remove Jabra personal devices from the **device inventory**. When you do so, you permanently remove the Jabra personal devices from **device groups**.

To remove a Jabra personal device from the device inventory:

1. On the left-hand navigation bar, click **Personal devices > Device inventory**
2. On the **Device inventory** table, check the checkbox next to the device you would like to remove
3. On the bottom ribbon, click **Delete**
4. In the **Delete device** dialog, click **Remove**

Note

Ensure that after you remove Jabra personal devices from the **device inventory**, you must also uninstall the **Jabra Plus Desktop** app from the end user computer(s) it was installed on.

Failure to do so means when the end user reconnects their Jabra personal device to their computer, the Jabra personal device is automatically re-added to the device inventory.

Adjusting settings remotely of a single Jabra personal device

The platform lets you remotely manage the settings of Jabra personal devices individually or in bulk.

If the Jabra personal device has an admin user-created configuration assigned to it, you *cannot* change the settings of a single Jabra personal device. To adjust the settings on a single device, the admin user can do so via the **device inventory**.

To adjust the settings of many Jabra devices at the same time, it is recommended to use [configurations](#) and choose a suitable approach. Be aware that when adjusting individual settings, the Jabra personal device must be online.

Tip

You can also use this procedure to test the settings of a single Jabra device before mass deployment and determine whether the changes are suitable or not.

To adjust the settings of one Jabra personal device:

1. On the left-hand navigation bar, click **Personal devices > Device inventory**
2. On the table of personal devices, find the Jabra device you would like to change settings for. You can search for the specific Jabra device using filtering based on *Model*, *Connection status*, *Device group*, *Firmware Status*, *Inactive devices*, or *Firmware Stage*
3. Click the Jabra device name, for example, Jabra Evolve3 85
4. Click the **Settings** tab, and adjust the settings of your relevant device
5. To apply the changes and deploy them to the end user, on the bottom ribbon, click **Publish changes**

For changes to take effect, ensure you restart the computer that the personal device is connected to. Changes are applied when the end user logs in to Windows® again.

Exporting the device inventory table or list

To see a list of your Jabra personal devices on a comma-separated values list, you can export your **device inventory** as a *.csv file. The list contains details such as *Firmware status*, *Computer name*, *Firmware version*, (device) *Serial number*, and others.

To export the list:

- On the **Device inventory** page, in the top right-hand of the list, click the action menu and then click **Export to CSV**. The file is then downloaded to your default *Downloads* folder associated with your web browser

Viewing Jabra personal device details

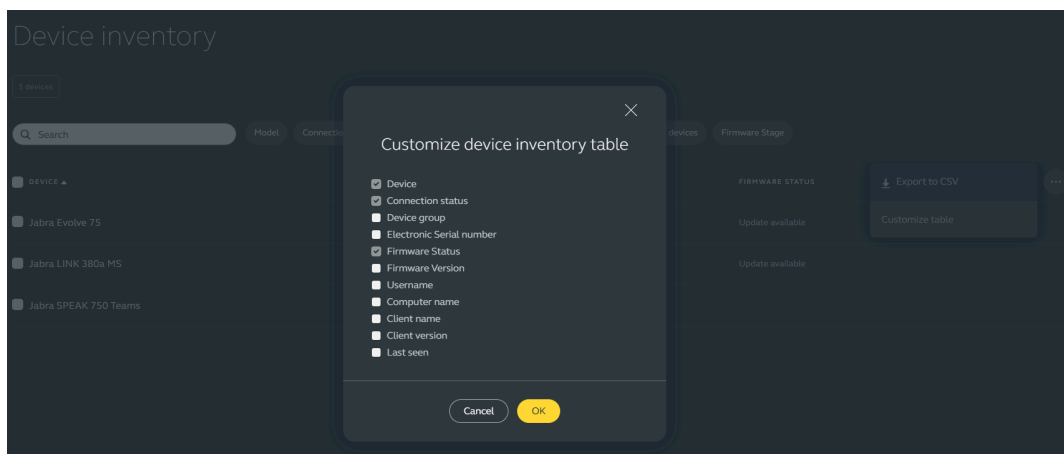
When a Jabra personal device is added to the **device inventory**, you can see information such as *Firmware status*, *Operating system*, *Computer name*, *Client version*, *Version Policy*, and others.

To do this:

- On the **Device inventory** page, click the device name on the list to see additional Jabra personal device details, such as Jabra Evolve3 85, Jabra Evolve2 75, etc. You can search for the specific Jabra personal device using filtering based on *Model*, *Device group*, *Firmware status*, or *Connection status*.

Customizing the device inventory table

You can customize your view of the **device inventory** and display or hide columns. Be aware that *Device*, *Connection status*, and *Firmware Status* remain selected and cannot be hidden or removed from the table.



To customize the device inventory table:

- On the **Device inventory** page, on the top right-hand side of the table, click the action menu and then click **Customize table**. In the *Customize device inventory table* dialog box, check or uncheck the checkboxes you would like displayed or hidden, and to save your preference, click **OK**

Device groups for personal devices

To help admin users manage and organize Jabra personal devices in the device inventory, **device groups** let the admin user sort the collection of Jabra personal devices into different containers or buckets. For example:

- Primary grouping: Organization (e.g., *ABC Company*)
 - Secondary grouping: Device groups (e.g., *Marketing, Human Resources*)

In this case, you can add Jabra personal devices from the **device inventory** into the individual **device groups** that were created and named. Device groups are essential for creating configurations, enabling the deployment of specific settings to select Jabra personal devices. See the *Configurations* chapter for details.

Creating a device group for personal devices

Creating a **device group** can be helpful when you have a large number of Jabra personal devices in your **device inventory** because it helps you create a container or bucket for them.

You can also create a device group to test a specific firmware version you would like to use with your Jabra devices, before you perform a mass deployment.

To create a device group:

1. On the left-hand navigation bar, click **Personal devices > Device groups**
2. On the **Device groups** page, click **Create**

3. In the **Create device group** dialog, in the *Name* field, enter a name for your device group, for example, *Marketing department*. Optionally, in the *Description* field, enter a description of your device group
4. Click the **Configuration** drop down to select the configuration you would like associated with the device group
5. Click **Create**

You are now taken to the **Device groups** page.

Sorting personal devices into a device group

After creating and giving a name to a **device group**, you can sort your Jabra personal devices into device groups.

A Jabra personal device can only be associated with one device group at a time. If the Jabra device is added to a different device group, the new one replaces the previous affiliation.

To sort Jabra personal device(s) from the device inventory to a device group:

1. On the left-hand navigation bar, click **Personal devices > Device inventory**
2. On the table, check the checkbox of the relevant Jabra device(s)
3. On the bottom ribbon, click **Add devices to device group**
4. In the **Add devices to device group** dialog, select a device group, and click **Add devices**

You have now added Jabra personal devices to a device group.

4.3 Meeting room device management

In the **Jabra Plus Management** platform, the **Meeting rooms** menu item enables you to visualize, sort, and manage Jabra meeting room devices, effectively mapping physical meeting rooms used for online meetings and creating an organizational structure.

Meeting rooms address the challenges of remote identification, management, and troubleshooting of Jabra meeting room devices. You can perform bulk management of settings and firmware, inspect real-time Jabra meeting room device or room status, reboot Jabra meeting room devices for troubleshooting, access activity logs for each meeting room, and other functionalities.

Like personal devices, Jabra meeting room devices have a virtual inventory, called **room inventory**. The **Meeting rooms** menu item is made up of the **Room inventory**, **Room configurations**, and **Room clients**.

When adding meeting room devices to the room inventory, there are two ways of approaching provisioning:

- **Adding during provisioning:** an admin user or AV Installer names the virtual room and adds the Jabra meeting room device, which appears in the **room inventory** as an *unassigned room*. The name helps identification (and can be changed anytime), letting you add the device first, then assign a room configuration and a firmware policy before moving the room to a location structure.
- **Adding before provisioning:** an admin user can add rooms first (name a room with an *Empty room* status), optionally assign a room configuration and/or firmware policy, then provision or add compatible Jabra meeting room devices and peripherals directly into those rooms. This strategy lets you create a room/location structure first before devices are provisioned – when delegating provisioning, the devices then appear in the correct room automatically.

For either provisioning approach, you can drag and drop these rooms into predetermined [locations](#), which serve as a grouping mechanism, similar to [device groups](#) (for personal devices). This is designed to hierarchically group or organize Jabra meeting room devices based on real or made-up locations e.g.: countries, cities, buildings, departments, rooms, or others.

The following is an example of a tree structure within locations.

Your organization (*root of tree structure*)

- **United States** (*Parent*)
 - **California** (*Child*)
 - **Cupertino office** (*Child*)

To keep Jabra meeting room devices updated with the latest firmware while minimizing disruptions for end users, you can modify [scheduled device updates](#) according to the organization's working hours. For example, updates can be scheduled to take place exclusively at night.

In the **room inventory**, clicking a Jabra meeting room device opens the **Room** page, displaying details such as *Room Type*, *Location*, *Software client*, and if applicable, *Room AV system*, *Video Service Provider*, and *Meeting room computer* or computing device information, among others.

Note

The *Video Service Provider* pane is displayed only in rooms with PanaCast 40/50/55 VBS meeting room devices. This also applies to PanaCast U30 when the meeting room device is connected to a controller/compute unit. Changing the video service provider between Microsoft® Teams Rooms and Zoom Rooms requires re-provisioning the affected meeting room devices.

Room inventory for meeting room devices

The **room inventory** is a repository or bucket for all Jabra meeting room devices added to a specific organization on the platform, like the [device inventory](#) for personal devices.

The room inventory enables you to set up a structure to organize your meeting rooms and Jabra devices in your business organization, showing you a real-time overview of your meeting room devices and status of your rooms.

Be aware that you can only have one room inventory per organization. All Jabra meeting room devices connected to the room client created by the same organization appear in the room inventory.

Through the **room inventory**, you can remove individual meeting room devices, or you can delete the entire room, removing any Jabra meeting room device within it.

Note

There are different procedures to remove Jabra meeting room devices from the **room inventory**. See the [Deleting a room or removing a meeting room device from a room](#) topic for procedures.

On a searchable and filterable list – the inventory outlines information such as *Room*, *Room Status*, *Location*, *Devices*, *Seat Count*, *IP Address*, *Configuration*, *Date added*, (Device) *Serial number*, and *Firmware Status*, all in real time.

Note

When a device serial number is not available, cannot be displayed or cannot be fetched from the device, be aware it is replaced by the **Electronic serial number**.

Room Status	Description
Connected	The room has Jabra meeting room devices that are <i>Online</i> and ready to use.
Disconnected	The room has Jabra meeting room devices, but they are <i>Offline</i> or not connected to power or the internet.
Empty	The room has been given a name and may have an assigned room configuration/firmware policy, but it has no Jabra meeting room devices connected to it. This room status also appears if you have removed or deleted all devices from the room.

In the **room inventory**, Jabra meeting room devices are first automatically sorted into **rooms** (a primary grouping), and rooms can be further sorted into **locations**, enabling you to create a secondary grouping for your rooms. For example, you can group rooms into different regions, countries, offices, and others, effectively building a hierarchical structure based on geography.

When Jabra meeting room devices are added to the room inventory – and to mass manage meeting room devices with a shared firmware policy and settings – a default **Standard Room Configuration** is applied across the board to all Jabra meeting room devices in the **room inventory**.

See [Standard Room Configuration](#) for further details.

Adding Jabra meeting room devices to the room inventory

To understand the different provisioning strategies, see the **Device provisioning methods and strategies** in the following topic [End of QSG – Next Steps](#). For provisioning procedures, see the [Device Provisioning & Onboarding Guide](#).

Moving a room into a location

To perform this procedure, you must first have created one or more locations in your **room inventory**. See the [Moving rooms into locations and adding room details](#) topic.

Adding a room

Depending on the [device provisioning method and strategy](#), an admin user can add a (empty) room to the **room inventory** to first create a room structure and then assign a room configuration/firmware policy to the room, before provisioning a meeting room device or peripherals to it.

Note

The Jabra meeting room device that requires a room client for provisioning i.e.: Jabra PanaCast 50 Room System, always appears as an *unassigned room* after provisioning, and cannot be added to a room.

For guidance, read the *Device provisioning methods* section in the [End of QSG – Next Steps](#) topic.

Creating a room structure first lets you use a *room provisioning code* so you can provision a Jabra meeting room device directly to a predetermined room. For more information on how to generate a *room provisioning code*, see the [Provisioning Codes](#) chapter.

To add a room to the room inventory:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** page, click **Add room**
3. In the **Select location** dialog, select the relevant location and click **Continue**
4. In the **Add a room** dialog, enter the Room name and click **Add**

You have now added a room with the status *Empty*. You must now [generate a room provisioning code](#) to add compatible Jabra meeting room devices to the room.

Adjusting settings remotely of a single Jabra meeting room device

The **Jabra Plus Management** platform lets you remotely manage the settings of Jabra meeting room devices individually or in bulk. You can only change the settings of a single Jabra meeting room device, when you have not assigned a custom room configuration to the room that includes the specific Jabra meeting room device. You can, however, adjust the settings on a single Jabra meeting room device via the **room inventory**.

Moreover, it is recommended that you [create a room configuration](#) to adjust the settings of many Jabra meeting room devices simultaneously. When adjusting individual settings, the Jabra meeting room device must be connected and online.

Tip

Prior to mass deployment, you can also use this procedure to test the settings of a single Jabra meeting room device.

To adjust the settings of one Jabra meeting room device:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** page, in your locations tree structure, click the name of your organization
3. On the **Room inventory** table, click the room name where your Jabra meeting room device is located
4. On the **Room details** page, click the relevant Jabra meeting room device pane
5. On the **Device details** page, click the **Settings** tab and make the necessary changes to settings
6. To apply the changes and deploy them to the end user, on the bottom ribbon, click **Publish changes**

After you click **Publish changes**, the setting changes are published or applied, and Jabra meeting room devices may automatically reboot.

Renaming a room

After provisioning a Jabra meeting room device, an admin user with the relevant permissions can rename the room.

To rename a room:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** table, click the room name you would like to rename
3. On the **Room** page, on the top right-hand side of the page, click the action menu (three-dot menu) and click **Edit room**
4. Rename the room as desired and click **Save changes** to confirm

Deleting a room or removing a meeting room device from a room

In **Jabra Plus Management**, an *owner* or *member with edit rights* (for meeting rooms) can delete rooms from the **room inventory** as well as remove a Jabra meeting room device from within a room.

Be aware that when you remove a room from the room inventory, you delete all Jabra meeting room devices within the room.

Depending on the Jabra meeting room device – and to permanently delete the room – you must ensure that after deleting a room or meeting room device from the room inventory, that you also uninstall the software client (room client) from the meeting room computer it was installed on.

If you do not delete the software client, when the meeting room computer is restarted, the Jabra meeting room device is automatically re-added to the room inventory as an *unassigned room*.

In the room inventory, when you remove a single meeting room device from a room, (i.e.: the structure created when the meeting room device was added to the platform) the room itself remains empty within the room inventory, ready to have a meeting room device provisioned to the inventory.

To remove a Jabra meeting room device from the room inventory, you must first ensure the *Device status* appears as *Offline* before removing it.

To do this, ensure that you unplug the Jabra meeting room device from the power outlet and wait a few minutes for the *Device status* to appear *Offline*. You can then perform the following procedure:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** table, click the relevant room name
3. On the **Room** page, on the card displaying the meeting room device, click the action menu, click **Remove device** and confirm
 - To remove the room entirely, including all the Jabra devices within the room, on the top right-hand side of the page, click the action menu and click **Delete room**

Important note

To permanently delete a room or Jabra meeting room device from a room, ensure that after you delete the meeting room device, you also [delete Jabra Plus clients](#) whenever possible.

Depending on the Jabra meeting room device, the client removal must be performed differently, and as follows:

- **PanaCast 50 BYOD:** After the meeting room device has been deleted from a room, or a room has been deleted, the PanaCast 50 BYOD is removed. To re-add the meeting room device to the platform, you must re-provision it.
- **PanaCast 50 RS:** After the meeting room device has been deleted from a room or a room has been deleted, you must switch the PanaCast 50 RS **OFF**, and the USB cable must be unplugged. To re-add the meeting room device to the platform, you must reinstall the Jabra Plus room client.
- **PanaCast U30** and **PanaCast 40/50/55 VBS:** After the meeting room device has been deleted from a room or a room has been deleted, the PanaCast U30 or 40/50/55 VBS is removed from the platform. To re-add the meeting room device to the platform, you must factory reset it and then re-provision the respective meeting room device.

Failure to remove the clients can result in the Jabra meeting room device being detected by the platform again and reappearing in the **room inventory**.

Activity logs – Device details and meeting room activity

Activity logs consist of device details and meeting room activities, allowing you to view information about Jabra meeting room devices and events in physical rooms.

From the **room inventory**, clicking a room name shows a timeline of activities related to that room and its associated meeting room devices. The **Activity** tab on each device's **Room** page lists events such as reboots, status changes, firmware updates, and errors.

Logs maintain a record of activities for the past 30 days, displayed in a searchable and filterable format, including **Events** in the room and their triggers (e.g., configuration changes or device additions/removals).

The **Activity** tab also shows the event and the exact time it occurred, impacted entity and admin user. For example, if an admin user renames a room, this action is logged.

Tip

Viewing additional **Details** and **Activity** aid troubleshooting by helping you identify the origin of issues, track actions, and resolve problems, such as rebooting the Jabra meeting room device.

Viewing Jabra meeting room device details

When a Jabra meeting room device is added to the **room inventory**, you can see information such as *Room name* and *Status*, *Location*, *Devices*, *Seat Count*, *Configuration*, and *Firmware Status*.

You can also find additional details of your Jabra meeting room device by drilling down into the **Device** page.

On the **Room** page, the **Room Details** tab displays **Room Information**, **Room Configuration**, **Room AV system / Meeting room computer**, **Date and Time** for scheduled device updates, and more.

The **Device Details** page shows you more granular information specific to the Jabra meeting room device, which includes *Installed Firmware* (version), *Firmware policy*, when the device was *Last Seen* as *Connected (Online)*, and more.

To view additional Room or Device details:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** page, in your **Locations** tree structure, click the name of your organization
3. On the **Meeting room inventory** table, click the relevant room name
4. On the **Room** page, click the **Details** tab to see more information about the room
 - To see more information about the Jabra meeting room device in the room, click the relevant pane on the **Room** page showing the Jabra meeting room device.

Viewing room activity

In addition to **Room Details** and **Device Details**, the **Activity** tab is a source of information that helps you track events and their triggers in a room.

The **Activity** tab captures events that occurred in a room, e.g.: *Firmware status*, *reboot*, *change of settings* of a meeting room device, and others.

To view activity in a room:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**

2. On the **Meeting room inventory** page, in your Locations tree structure, click the name of your organization
3. On the **Meeting room inventory** table, click the relevant room name
4. On the **Room** page, click the **Activity** tab

The activity log in a room (and the meeting room devices within) is now visible on a list that can be sorted by *Time*, *Impacted Entity*, *Event*, and *User*.

Locations

Locations are a secondary grouping, designed as a hierarchical tree structure to sort and organize your organization's virtual meeting rooms and meeting room devices. It is located within the **Room inventory** menu item.

You can use locations as a geographical representation of your organization with individual rooms within each location. If you have created a location-based hierarchy, be aware that you can drill down several levels in the hierarchical structure. You can also optionally [restrict or limit access to the room inventory](#) of that location, for certain admin users.

A location consists of a name and a placement in the hierarchy that you choose. The following examples illustrate an organization with a simple hierarchical structure and a more complex one. Be aware that your organization may be simpler and may not need many locations.

In these examples, certain rooms do have Jabra devices provisioned, while others are just an *empty room without devices* provisioned to it.

In the example that follows, **ABC Company** is your organization, **First floor** and **Second floor** rooms are a location you created, and within these locations you have the different rooms in your organization (e.g., Room 100, Room 101, Room 102) that you created before or during provisioning.

ABC Company (your organization)

- **First floor meeting rooms**

- Room 100
 - *Jabra meeting room device A*
- Room 101
 - *Jabra meeting room device B*
- Room 102
 - *No device provisioned yet (empty room)*

- **Second floor meeting rooms**

- Room 200
 - *Jabra meeting room device C*
- Room 201
 - *No device provisioned yet (empty room)*
- Room 202
 - *Jabra meeting room device D*

Adding, renaming, or deleting a location

You can also add, rename, or delete a location in the **room inventory**. Like a parent-child hierarchy, when you add a location starting from the top of the tree structure, you can create as many locations as the organization may need.

Moreover, when you create more locations within the nested groups you can have up to six levels of hierarchy. You can also rename or delete a location.

Adding a location:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the left-hand side of the screen, on the locations tree structure, click the action menu (three-dot menu) and then click **Add location**
3. In the **Add location** dialog, in the *Location name* field, enter the name of the new location, and click **Create**. The new location appears beneath the location that you chose to group it under.

Renaming a location:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the left-hand side of the screen, on the locations tree structure, click the action menu (three-dot menu) of the relevant location you would like to rename, and then click **Rename**
3. In the **Rename location** dialog, in the *Name* field, enter the new location name
4. Click **Save**. The location has now been renamed.

Deleting a location:

Note

Be aware that when you delete a location you also delete all the *children* locations beneath.

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**

2. On the left-hand side of the screen, on the locations tree structure, click the action menu (three-dot menu) of the relevant location you would like to delete, and then click **Delete**
3. In the dialog that appears, click **Delete** to confirm. The location is now deleted.

Moving rooms into locations and adding room details

After provisioning meeting room devices, an *unassigned room* is created in the locations tree structure, within the **room inventory**. You can move the unassigned room into a predetermined location that you may have created in the tree structure.

Note

If you use the *room provisioning code*, there is no unassigned room created, as the room is created during the provisioning of the meeting room device.

Moreover, when you move a room into a location, an **Add details** dialog appears, letting you add room information such as *Room name*, *Seat Count*, *Description*, and others.

Tip

The following procedure is also helpful when you have already provisioned several Jabra meeting room devices into the platform as *unassigned rooms*, and you would also like to [bulk assign a room configuration](#) that you have previously created or change room names.

To do this:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** page, click *unassigned room*
3. On the list of *unassigned rooms*, drag and drop the room into the desired location in the hierarchical structure
4. In the **Add details** dialog, if necessary, enter the relevant information in the provided fields, and then click **Save**

Scheduling firmware updates for meeting room devices

See the [Scheduled device updates](#) topic in the firmware management chapter.

4.4 JabraCLI - Offline device management

In Jabra Plus Management, you can download a model configuration of (a) personal device(s) or a room configuration for a meeting room device as a ***.JSON** file, which you can then use to manage, configure and update Jabra devices offline without having to use the Jabra Plus Management platform, via JabraCLI.

For setup documentation and guidance on how to use JabraCLI, including supported devices and commands, see the README.MD file included in JabraCLI that you can download from [Jabra for Developers](#).

Exporting a configuration

You can export and download a previously created configuration, if you have the relevant permissions. Be aware that anyone with access to the platform (*Owners or Members*) can export a configuration or room configuration.

To export and download a model or room configuration, (including its firmware policy, for meeting room devices):

1. On the left-hand navigation bar, click **Personal devices > Configurations**
 - a. For meeting room devices, click **Meeting rooms > Room configurations**
2. On the **Configurations** or **Room configurations** page, select the configuration you would like to export
3. Click the **Export** tab
4. In the **Export room configuration for JabraCLI** pane, click the **Download JSON** button and when prompted, save it to the folder of your choice

You can now use the ***.JSON** file to manage Jabra devices offline.

4.5 Integrating with other software

4.5.1 Integrating other software with Jabra Plus Management

Important note

Integrations in **Jabra Plus Management** is currently in a *beta* state and some functionality may be added or removed before the final release.

During this period, you can grant API access for asset management (Jabra meeting room and personal devices) and create configurable webhooks for Jabra meeting room devices.

For technical support during the beta period, developer documentation and procedures refer to [Jabra for Developers](#).

Jabra Plus Management's **Integrations** menu item enables admin users to connect the platform with their own external software systems, allowing them to specify where to send Jabra meeting room device events, and manage API access to the API portal for asset management of personal and meeting room devices.

This lets your organization consume Jabra device data for workflows, real-time monitoring, or automation.

Integrations is currently *beta* and is visible only to certain admin users in **Jabra Plus Management**.

Who can access Integrations

- Only admin users with the *Owner* role can view and use Integrations.

What you can do with Integrations

- Push device events to external systems using webhooks in near real-time and receive real-time updates without polling.
- Configure, manage and add multiple webhook endpoints and control which events are sent to each.
- Grant or revoke access to the Jabra API portal via the platform to any user so they can use APIs to read device inventory, perform supported management actions and telemetry (e.g.: Device information, device settings, firmware, remote reboot, and others).
- Combine webhook (push) and API (pull/command) approaches to integrate Jabra device data and workflows into custom applications.
- Use integrations to automate follow-up actions (for example: create a ticket, update an asset record, trigger an alert) when specific device events occur.

Adding a webhook for Jabra meeting room devices

You can add a webhook to send event data from Jabra meeting room devices to other services and platforms.

To do this:

1. On the left-hand navigation bar, click **Integrations**
2. On the **Configurable Webhooks** tab, click **Add webhook**
3. In the **Add webhook for meeting rooms** dialog, in the **Name** field, enter a name
4. In the **Webhook URL** field, enter the URL
5. In the **Authentication method** dropdown, select the desired method
 - Optionally, you can check the **Include device status changed** checkbox, and/or the **Include device firmware changed** checkbox.
 - Optionally, you can also click **Download schema**, to download a *.JSON file that shows the structure of the webhook data.
6. Click **Add webhook**

Granting API access

You can grant any user access to Jabra Plus APIs to integrate Jabra device functionality into your cloud service.

To do this:

1. On the left-hand navigation bar, click **Integrations**
2. On the **API Access** tab, click **Grant API access**
3. In the **Grant API access** dialog, in the **First name**, **Last name**, and **Email address** fields, enter the user's relevant information
4. Click **Grant access**

Viewing primary and secondary keys

You can view the primary and secondary keys to share them with a developer for API integration.

To do this:

1. On the left-hand navigation bar, click **Integrations**
2. In the **Integrations** page, on the list of users with API access, click the action menu (three-dot menu) and click **View and edit details**
3. In the **Grant API access** dialog, click the upper (primary) field or the lower (secondary) field, and copy the primary and/or secondary key to your

clipboard

4. Close the dialog

5 Configurations

A configuration is a collection of settings that includes firmware management for Jabra meeting room and personal devices.

When adding a Jabra device to the platform, a default configuration with Jabra-recommended settings is automatically applied. A configuration includes a default firmware policy. See the [firmware management](#) topic for guidance.

The **Standard Configuration** and **Standard Room Configuration** are the defaults for all Jabra meeting rooms and personal devices in the organization, respectively.

In the **Configurations** or **Room configurations** menu item, admin users can set exceptions for specific Jabra device models that apply to either all Jabra meeting room devices in the physical meeting rooms or all Jabra personal devices.

Note

Setting exceptions overwrites and modifies the **Standard Configuration** or **Standard Room Configuration**.

For example, admin users can designate a group of Jabra personal devices that require a specific setting or a specific firmware version; This can be achieved when you create a **device group** and then create a custom configuration and then assign it to the device group.

For Jabra meeting room devices, **room configurations** can be created to tailor specific room experiences. For example, you can select specific Jabra meeting room device models, customize the available model settings, and then assign or bulk assign the room configuration to rooms in the **room inventory**.

Additionally, you can [duplicate configurations](#) or create configurations with customized [firmware policies](#), ensuring that all Jabra devices in the organization benefit from the latest firmware releases.

5.1 Configurations for Jabra personal devices

It is recommended that the configuration approach chosen by an admin user is based on the level of complexity for firmware and settings management.

The following are three approaches to configuring Jabra personal devices on the platform:

- **Standard Configuration:** This is the default configuration. This approach is suitable when the admin user wants the same configuration applied to all Jabra personal devices in the organization's **device inventory**. Therefore, the **Standard Configuration** affects all personal devices that are not part of a **device group**, and applies immediately and automatically to the entire organization, ensuring all Jabra personal devices are continuously updated to the latest firmware versions, effectively deploying an organization-wide firmware policy.
- **Exceptions:** You can set exceptions to the Standard Configuration when all Jabra personal device models require the same configuration settings, with some specific exceptions. This approach lets you set a specific setting for a specific Jabra personal device model across the board.
- **Create configuration:** In this approach you can create a custom configuration to apply specific settings to one or many groups of Jabra personal devices and determine their firmware policy. With this approach, you can effectively replace the **Standard Configuration** for a group of specific Jabra personal devices with the settings that were previously chosen in the custom configuration. Another way to use a custom configuration is to test a Jabra personal device setting on a group of specific Jabra device models before mass deployment.

Setting exceptions to the Standard Configuration

You can edit the **Standard Configuration** and set exceptions for Jabra personal device model settings, such as firmware management (e.g.: force a specific Jabra personal device model to use a predetermined firmware) or device settings management. The exception(s) are then applied automatically to the **device inventory**.

For example, you may have an organization where specific settings need to apply to a model range of Jabra Evolve3 85 personal devices, such as a low or high *Sidetone* level, *Wearing detection*, or other settings. With this approach, all Jabra Evolve3 85 personal devices in the organization automatically apply the setting.

To do this:

1. On the left-hand navigation bar, click **Personal devices > Configurations**
2. On the **Configurations** page, click the **Standard Configuration** pane
3. On the **Standard Configuration** page, click the **Model Configurations** tab
4. On the top right-hand side of the page, click **Add model** and select the relevant Jabra personal device, for example, Jabra Evolve3 85
5. On the bottom ribbon, click **Continue**

6. On the **Manage settings** page, adjust the settings. You can also lock specific settings for end users by toggling the relevant switches
7. To apply the changes, on the bottom ribbon, click **Publish** and in the **Publish model settings** dialog, click **Publish** again to confirm

For changes to take effect, ensure you restart the computer that the personal device is connected to. When the end user logs in to Windows® again, the changes are applied.

Walkthrough: Creating and assigning a configuration for personal devices

Note

This walkthrough is best suited for admin users in organizations with specific requirements for their Jabra personal device models.

This walkthrough lets you create a custom configuration for specific Jabra personal device models; This requires more effort and adds complexity when managing Jabra personal devices remotely.

In this approach, **device groups** play an important role because you deploy and manage Jabra device model configuration or settings for each group of Jabra personal devices (instead of all Jabra personal devices in the **device inventory**).

An example of when you would create a custom configuration is in a call center scenario or an open office setting, where a group of people using Jabra headsets would prefer a quieter environment.

In this case, the admin user creates a configuration whereby the *Sidetone* feature (*audio feedback from the person's own voice to improve a call experience*) is adjusted accordingly, letting headset users hear themselves when speaking on the headset microphone.

Be aware that when you delete an assigned configuration, Jabra personal devices are automatically re-assigned the [Standard Configuration](#).

To begin the walkthrough, perform all procedures from A to D:

A. Creating a device group

Before you can assign a configuration to Jabra personal devices, [you must create one or many device groups](#). Afterwards, the admin user must add the Jabra personal device(s) to the device group.

B. Adding Jabra devices to the device group

After creating a **device group**, the admin user must add or sort the Jabra personal device(s) to the device group, and then continue with creating a configuration that applies to Jabra personal devices in the device group.

C. Creating a configuration

To assign specific settings to a group of Jabra personal devices in a **device group**, you must first create a configuration.

Tip

After you create and save your configuration, you can optionally duplicate the customized configuration and use it for other device groups you may have. For the procedure, see the [Duplicating a configuration for personal or meeting room devices](#) topic.

To create a configuration:

1. On the left-hand navigation bar, click **Personal devices > Configuration**
2. On the **Configurations** page, click **Create**, and in the **Create configuration** dialog, in the fields provided, enter a **Name** and optionally a **Description** and click **Create**
3. In the **Add model configuration** dialog, click **Add models**

Note

When you click **Skip adding models**, you can perform the following steps from the **Configurations** menu item later.

4. To select models, find the Jabra personal devices you want to assign a configuration to, and check the checkbox of the relevant Jabra device models and when you are finished, on the bottom ribbon, click **Continue**
5. On the **Manage settings** page, adjust the settings for the chosen Jabra personal device model. When you are finished, on the bottom ribbon, click **Publish**, and to confirm, click **Publish** again

Tip

When selecting multiple models, the **Publish** button changes to **Next model** so you can seamlessly configure all models within the configuration.

For changes to take effect, you must assign a configuration to a **device group**. Optionally, before you assign a configuration, you can lock settings for end users for Jabra personal devices in a device group. For the procedure, see the [Locking settings](#) topic.

D. Assigning a configuration to a device group

After creating a custom configuration for Jabra personal devices, you must assign it to a **device group**. See the procedure on [Assigning a configuration to a device group or a room](#).

5.2 Room configurations for Jabra meeting room devices

With room configurations, an admin user can mass manage Jabra meeting room devices with a shared firmware policy and settings as soon as they are added to the [room inventory](#).

Changing **model settings** for your Jabra meeting room devices lets you configure the room experience depending on the size and typical usage of a physical room.

The room configuration approach you choose is based on the level of complexity of your firmware and settings management. **Standard Room Configuration** is the least complex approach and the most recommended.

An admin user can also set exceptions to the **Standard Room Configuration**, or the most complex approach is when you [create a room configuration](#) from the ground up.

Note

As changes are implemented, Jabra meeting room devices may automatically [reboot](#) unless they are on an active call.

The following are approaches to configuring your Jabra meeting room devices on the platform:

- **Standard Room Configuration:** This is the default room configuration and is suitable when you want the same **room configuration** applied to all Jabra meeting room devices that appear as rooms in the **room inventory**. Choosing **Standard Room Configuration** affects all Jabra meeting room devices not assigned to a custom room configuration, and it applies immediately and automatically to the entire organization (irrespective of the location) ensuring all Jabra meeting room devices follow the same firmware policy and Jabra-recommended model settings.

- **Exceptions:** In the **Standard Room Configuration**, you can set model exceptions to set the same room configuration settings for all their Jabra meeting room devices, with specific exceptions applied to a Jabra meeting room device model configuration. For example, an *owner* or *member with edit rights* (for meeting rooms) can modify the default Jabra-recommended model setting for *Automatic Zoom mode* on the PanaCast U30; this exception replaces the default setting for *Automatic Zoom mode* on all PanaCast U30 meeting room devices that are provisioned to the **room inventory**.

Note

When setting exceptions or creating a room configuration, you must select the corresponding Jabra meeting room device model, for example, when you add a model configuration for the PanaCast 50 RS or PanaCast 50 BYOD, you must select the **PanaCast 50** option.

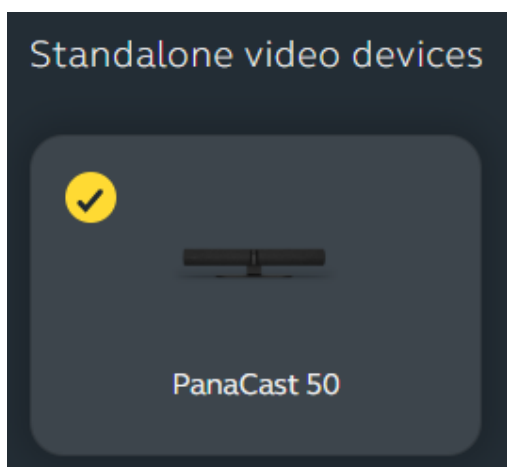
When you have a PanaCast 40/50/55 VBS, you must select one of the **PanaCast Video Bar System** options (i.e. the video service provider MTR, ZR or BYOD), however, there are exceptions. See the [Firmware bundles and specific firmware versions](#) topic for guidance.

- **Create room configuration:** In this approach, you can create a custom room configuration to apply specific settings to one or many rooms with Jabra meeting room devices and determine their firmware policy. With this approach, you effectively replace the **Standard Room Configuration** for specific rooms and their associated Jabra meeting room devices with the previously chosen settings, enabling you to configure Jabra meeting room device model variants that can be assigned to rooms depending on the room type or typical usage.

Setting exceptions in the Standard Room Configuration

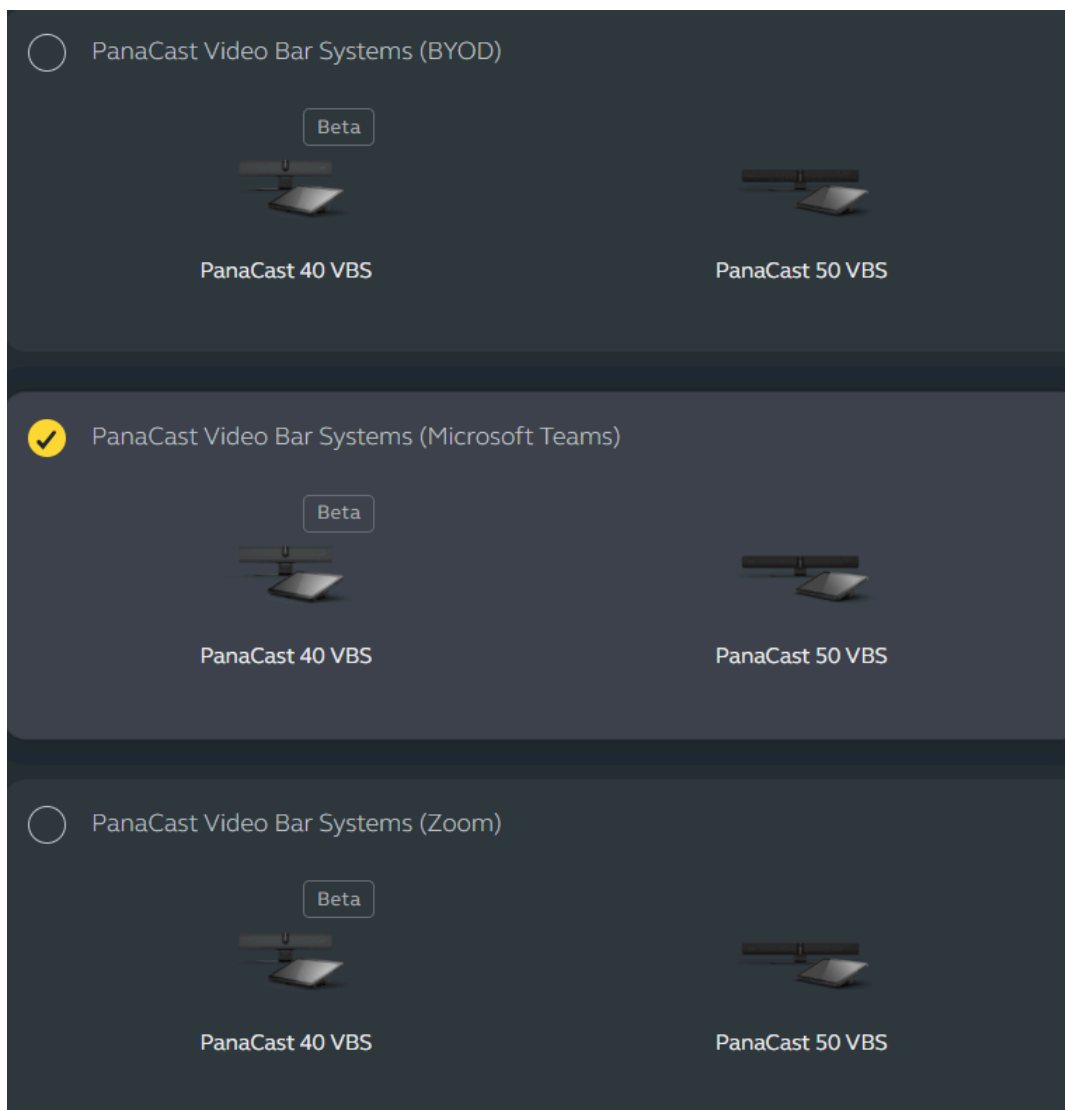
An admin user can edit the **Standard Room Configuration**, set exceptions for specific Jabra meeting room device models or set exceptions for device model configurations, settings and firmware. For firmware updates, see the [firmware management](#) chapter.

When you have both PanaCast 50 Room System (RS) and PanaCast 50 – Bring Your Own Device (BYOD) in your organization's **room inventory**, and want to set an exception to either PanaCast 50 RS or PanaCast 50 BYOD, you must [create a room configuration](#) selecting the **PanaCast 50** card, and assign it to the rooms where the specific PanaCast 50 RS or PanaCast 50 BYOD are located.



Depending on the video service provider that you chose during provisioning for your PanaCast 40/50/55 VBS, when selecting models in a configuration, ensure you select the matching card, as each variant has *their own* collection of model settings.

For example, if you have a PanaCast 55 VBS and during provisioning you select the Microsoft® Teams variant as video service provider, ensure you select the **PanaCast Video Bar Systems (Microsoft Teams)** card.



The exception(s) are applied automatically to all Jabra meeting room devices in the **room inventory** for the specified Jabra meeting room device model. The default Jabra recommended setting(s) for your Jabra meeting devices are then replaced by the model setting(s) you set.

To set an exception in the Standard Room Configuration:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**
2. On the **Room configurations** page, click the **Standard Room** pane
3. On the **Standard Room** page, click the **Model Configurations** tab
4. On the top right-hand side of the page, click **Add model** and select the relevant Jabra meeting room device model
5. On the bottom ribbon, click **Continue**
6. On the **Manage settings** page, adjust the setting you would like to set as an exception

7. To apply the changes, on the bottom ribbon, click **Publish**, and in the **Publish model settings** dialog, click **Publish** again to confirm

Settings are published or applied now, and your Jabra meeting room devices may automatically reboot.

Walkthrough: Creating and assigning a room configuration

Note

Creating custom room configurations is best suited for an organization with specific requirements for their Jabra device models.

This walkthrough lets you create custom room configurations for specific Jabra meeting room device models and assign the custom room configuration to one or many specific rooms. This requires more effort and adds complexity when remotely managing Jabra meeting room devices.

The added complexity, however, enables you to fine-tune the settings of the Jabra meeting room devices to create a customized experience for a specific type of meeting room.

A sample use case for creating a room configuration can be as follows: In an organization, you may have a small room that fits a seat count of two and is typically used for face-to-face meetings. In this case, you can create a configuration, whereby the *Field of view* setting is adjusted accordingly from the default 180° to a custom 120°.

In the walkthrough that follows, you can deploy and manage settings for a specific Jabra meeting room device model within a room, instead of all Jabra meeting room devices in the organization's **room inventory**.

To begin the walkthrough, continue with both the A and B procedures that follow:

A. Creating a room configuration

To create a room configuration:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**
2. On the **Room configurations** page, click **Create**, and in the **Create room configuration** dialog, in the fields provided, enter a **Name** and optionally a **Description** and click **Create**
3. In the **Add model configuration** dialog, click **Add models**

Note

When you click **Skip adding models**, you can perform the following steps from the **Room configurations** menu item later.

4. To select the specific meeting room device models on the list, find the Jabra meeting room devices you would like to assign a configuration to, and check the checkbox of the relevant Jabra meeting room device, and on the bottom ribbon, click **Continue**
5. On the **Manage settings** page, adjust the settings for the chosen Jabra device model(s). When you are finished, on the bottom ribbon, click **Publish**, and to confirm, click **Publish** again.

For changes to take effect and to finish this walkthrough, the next step is to assign the room configuration to a room. Optionally, before you assign an already created room configuration, you can also see the [locking settings](#) for specific Jabra meeting room device models in a room procedure.

B. Assigning a room configuration to a room

You have created a custom room configuration and must assign it to a room. See the procedure [Assigning a configuration to a device group or a room](#).

5.3 Assigning a configuration to a device group or a room

For a configuration that you customized to take effect on a group of Jabra personal devices and replace the default **Standard Configuration** for the group of Jabra devices, you must change the assigned configuration of the **device group**.

For the previously customized room configuration to take effect, you must assign the configuration to a room in your [room inventory](#) or a room that you have grouped into a [Location](#). Optionally, to [bulk assign a room configuration to many rooms](#), see the procedure in the appendix.

- **For Jabra personal devices**

To assign a configuration to a device group:

1. On the left-hand navigation bar, click **Personal devices > Device groups**
2. On the **Device groups** page, find and click the relevant device group pane
3. On the top right-hand side of the screen, click the action menu (three-dot menu) and click **Change configuration**
4. In the **Change configuration** dialog, in the drop-down menu, select the configuration name you created, and click **Apply**

For changes to take effect on the Jabra personal devices in a device group, ensure you restart the computer that the Jabra personal device is connected to. Changes are applied when the end user (of the Jabra personal device) logs in to Windows® again.

At this point, you have now assigned a custom configuration to a device group.

- **For Jabra meeting room devices**

To assign a room configuration to a room:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** table, click the relevant room name
3. On the **Room** page, in the **Room configuration** pane, click the pencil icon (edit menu)
4. In the **Change room configuration** dialog, in the drop-down menu, select the name of the configuration you previously created, and click **Apply** to confirm

After you click **Apply**, settings are published or applied, and your Jabra meeting room devices may automatically reboot. In the case of firmware management, any pending firmware updates are performed based on the schedule for device updates.

At this point, you have now assigned a custom room configuration to a room.

5.4 Settings lock for Jabra device models

You can lock specific settings that affect specific Jabra meeting room or personal device model(s) in their respective inventories or can also lock settings in a configuration that is assigned to either a room or **device group**.

Locking a setting ensures that when different admin users adjust settings remotely of a single Jabra meeting room device or a single Jabra personal device, the other admin users can only change settings that have *not* been previously locked.

When you set **exceptions** to the **Standard Configuration** or **Standard Room Configuration** and want a specific setting to apply as a locked setting for a Jabra meeting room or personal device model, you are locking settings for all Jabra meeting room or personal devices of a model variant, globally.

For example, your business may follow a specific audio or hearing protection standard, and you want to lock this setting, globally. In this case you can apply and deploy the *Hearing Protection* setting as a locked setting in the **Standard Configuration** or **Standard Room Configuration**.

You can also lock settings for a specific meeting room device model in a specific room only, to do this, see the [locking settings for Jabra meeting room devices in specific rooms](#) topic.

On the other hand, to lock settings for a specific Jabra personal device variant in a specific device group, see the topic [locking settings for end users for Jabra personal devices in a device group](#).

Locking settings for specific Jabra device models globally

You can lock settings for specific meeting room device *models* in the **Room configurations** menu item and/or lock settings for specific personal devices in the **Configurations** menu item.

For example, the locked settings can apply to all PanaCast U30 located within the entire **room inventory** or can apply to all Jabra Evolve3 85 headsets within the entire **device inventory**.

The locked settings apply to all devices in the **room inventory** or **device inventory**.

To lock settings for a specific Jabra meeting room device model or personal device globally:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations** or **Personal devices > Configurations**
2. Click the **Standard Room** pane or **Standard Configuration** pane
3. On the upper-right-hand side of the page, click the **Add model** button
4. On the list, click to select the model name of the relevant Jabra meeting room or Jabra personal device, and then click **Continue**
5. On the **Manage settings** page, toggle the relevant switches on the settings that you want to lock



6. To apply the locked settings, on the bottom ribbon, click **Publish**, and in the **Publish model settings** dialog, to confirm, click **Publish** again

After you click **Publish**, settings are applied immediately, and Jabra meeting room devices may automatically reboot.

Locking settings for Jabra meeting room devices in specific rooms

You can lock settings for a Jabra meeting room device in a specific room. For example, the locked settings can apply only to a PanaCast U30 within a specific room.

To lock settings for a Jabra meeting room device in a specific room:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**
2. Click the **Room configuration** pane that you have previously created
3. On the top right-hand side of the page, click the **Add model** button, and on the list, select the name of the relevant Jabra meeting room device, for example, PanaCast U30, and then click **Continue**
4. On the **Manage settings** page, toggle the **Lock for end user** switch for the setting that you want to lock



5. On the bottom ribbon, click **Publish**, and in the **Publish model settings** dialog, click **Publish** again to confirm
6. To assign the locked settings, on the left-hand navigation bar, click **Meeting rooms > Room inventory**, find the relevant room name and in the **Room configuration** pane, click the pencil icon (edit menu)
7. In the **Change room configuration** dialog, in the drop-down menu, select the name of the configuration with the locked setting(s), and click **Apply** to confirm

After you click **Apply**, settings are published immediately, and your Jabra meeting room devices may automatically reboot.

Locking settings for Jabra personal devices in a device group

You can also lock settings for one or a group of specific Jabra personal devices within a **device group**.

For example, locked settings can apply to specific personal device models, such as Jabra Evolve3 85 headsets, Jabra Engage 40 Stereo, whereby the first model would always have *Sidetone* switched **ON**, while for the other model it is switched **OFF**.

To lock settings for Jabra personal devices in a device group:

1. On the left-hand navigation bar, click **Personal devices > Configurations**

2. On the **Configurations** page, find and click the pane with the previously created configuration, and on the upper-right-hand side of the page, click the **Add model** button
3. From the list of Jabra device models, click the relevant device or devices (for example, Jabra Evolve2 65 and/or Jabra Evolve3 85), and then click **Continue**
4. On the **Manage settings** page, find the setting you would like to lock, and toggle the **Lock for end user** switch



5. On the bottom ribbon, click **Publish** and to confirm, click **Publish** again.
 - If you selected more than one personal device in step three, click **Next model** and lock the desired setting(s)
6. To assign the configuration to a device group, on the left-hand navigation bar, click **Personal devices > Device groups** and then click the device group pane you would like to assign the configuration to, and on the top right-hand side, click the action menu and then click **Change configuration**
7. In the **Change configuration** dialog, in the drop-down menu, click to select the configuration name where you locked settings and click **Apply**

Settings are locked the next time an end user restarts their computer with the connected Jabra personal device.

6 Firmware management

You can remotely manage firmware and policies for Jabra personal and meeting room devices via the platform.

- **For Jabra personal devices:** Firmware updates are performed through the **Jabra Plus Desktop** app. Admin users can select specific firmware versions for device models, applying them across inventories or device groups, as well as in exceptional cases, downgrading firmware. If a firmware update fails, a recovery process is available for wired devices via the app. End users receive prompts to update firmware based on organizational policies or can postpone them.
- **For Jabra meeting room devices:** Firmware is managed directly on the platform, allowing updates or downgrades per organizational policies. Updates are pushed directly to the meeting room devices and follow a [schedule for device updates](#). Without a defined schedule, updates may interrupt meetings, as devices must reboot.

Important note

Jabra may cease support for certain firmware versions due to compatibility issues, security vulnerabilities, or regulatory changes. When a previously selected firmware version becomes unsupported, the affected Jabra devices continue to operate normally. However, subsequent Jabra devices added to the respective inventories keep their existing firmware and cannot update to the unsupported version.

When a specific firmware version is no longer supported by Jabra, in the **device inventory** or **room inventory** an exclamation mark (!) indicates the affected Jabra devices. Additionally, a *Configuration warning* appears in the affected configuration or room configuration. For details, see the [Troubleshooting](#) section.

The end user may continue to use the Jabra device with the unsupported firmware; however, the Jabra device's settings can no longer be changed, and it is therefore not recommended, as it may cause undesired behavior.

To resolve this, an admin user on the platform with the relevant permissions must edit the configuration to either select a different firmware version or switch the toggle to *Always use latest* **ON**, automatically updating the Jabra device to the latest firmware.

To select a different firmware version, see the procedure [Modifying & setting the firmware policy for specific Jabra device models](#). If you have configurations assigned to a specific room or Jabra personal devices in a device group, see the [Modifying & setting an existing firmware policy for a specific Room or device group](#) procedure.

Firmware policy & updates

The firmware policy — contained within [Configurations](#) — enables you to manage firmware for Jabra devices in the **Jabra Plus Management** platform, giving end users access to the latest updates and features for their Jabra device.

Note

Certain older Jabra devices' firmware cannot be updated via **Jabra Plus**. Instead, they must be updated using **Jabra Direct** or **Jabra Xpress**.

You can still use the older Jabra devices in **Jabra Plus** and change settings, however, depending on the firmware version you are running, the list of settings that you can modify in **Jabra Plus** can change.

To find out whether your device can be firmware updated or not, see the [list of supported Jabra devices](#).

Governed by a firmware policy, you can control and enforce firmware deployment of the latest firmware updates on all Jabra devices (in their organization) or set exceptions for specific Jabra device models, for example, preventing updates to all Jabra Evolve3 85 personal devices or restricting all PanaCast U30 to use a particular firmware version.

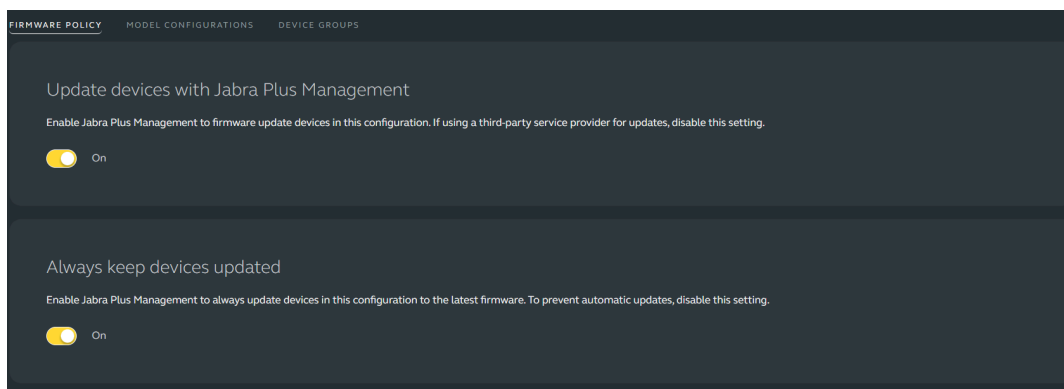
The default firmware policy is part of the **Standard Configuration** or **Standard Room Configuration**, as well as any customized **configuration**. The default firmware policy applies in both cases, however, the default works differently for Jabra meeting room and for personal devices.

Modifying the default firmware policy effectively creates a custom policy, but these cannot be named as they are contained within configurations.

Therefore, to have different firmware policies for various Jabra device models, an admin user must first [create a configuration](#) or [create a room configuration](#) and then modify the firmware policy accordingly.

For both Jabra meeting room and personal devices, a firmware policy consists of the following toggle switches:

- **Update devices with Jabra Plus Management:** primary toggle switch that enables or disables Jabra device firmware management on the platform
- **Always keep devices updated:** secondary toggle switch that updates all Jabra devices to the latest firmware version when available



Also, the default firmware policy acts differently according to the type of Jabra device, and as follows:

- **Personal devices:** the default setting for both toggle switches is **ON**, which means firmware is managed automatically, and end users are notified of updates via **Jabra Plus Desktop** app. However, you can disable the firmware policy to prevent updates and keep the currently installed firmware version.
- **Meeting room devices:** the default setting for the firmware management toggle is **OFF**, meaning firmware is not managed through the platform. Consequently, updates are not automatically applied.

Note

When you enable firmware updates in the **Jabra Plus Management** platform, you must disable firmware updates from other platforms, such as **Windows® Update**.

This means whenever a Jabra meeting room device is added to the **room inventory**, you can manage the firmware exclusively within the platform.

You can modify & set the firmware policy for specific Jabra device models in the [Standard Configuration](#) for all personal devices in the **device inventory**. You can also set a specific firmware version for a Jabra meeting room device model in the [Standard Room Configuration](#) that is automatically assigned to all your meeting room devices in the **room inventory**.

Moreover, in any [custom configuration](#) that was saved and assigned to specific **device groups**, as well as any [custom room configuration](#) that was saved and assigned to specific rooms, you can modify & set a firmware policy for a specific room or device group. You can also restrict the **Always use latest firmware** feature only to a specific Jabra device model.

Both inventories show *Firmware status* for all rooms and personal devices. See the [Firmware Statuses](#) topic for guidance.

Firmware Statuses

On the platform, the status of firmware updates is located within the **device inventory** or **room inventory**, and the statuses differ depending on personal or meeting room devices.

Shown in Device or Room inventories	Description
Postponed update ¹	The firmware update installation of the Jabra device has been delayed or postponed to a later time or date by the end user.
Failed update	The firmware update installation of the Jabra device has failed on the end user computer. The end user can recover the Jabra device and retry the firmware update. Depending on the error code, the failed update can retry the update on its own.
Pending update	Waiting for the end user to perform the firmware update. It can also occur if the Jabra device is <i>Offline</i> .
Latest installed	The installed firmware version being the most recent release, which includes the latest improvements, features and bug fixes. This message is also displayed when firmware management is disabled.
Update available ¹	A new firmware version is available but has not yet been configured by you, the admin user. On the other hand, the end user is notified of an update to their Jabra device in the Jabra Plus Desktop app. Can also be shown when the Update devices with Jabra Plus Management Toggle is switched OFF.
Update scheduled ²	Specific date and time set in the Jabra Plus Management platform when the update takes place. See the Scheduled device updates topic.

¹ Jabra personal devices only

² Jabra meeting room devices only

Enabling or disabling firmware management for Jabra devices

In the **Jabra Plus Management** platform, you can remotely manage firmware for Jabra personal and meeting room devices, respectively.

- **Meeting room devices:** The default firmware policy for meeting room devices applies automatically to the **Standard Room Configuration** and is switched **OFF** (disabled) by default.

To enable firmware management, you must first decide to **Update devices with Jabra Plus Management** (primary toggle switch) **ON** and then decide whether to switch **ON** the **Always keep devices updated** (secondary toggle switch) to update all Jabra meeting room devices to the latest firmware version when available.

- **Personal devices:** For Jabra personal devices, the default firmware policy applies automatically to the **Standard Configuration**, which is switched **ON** (enabled) by default.

When enabled, firmware-related notifications are sent via **Jabra Plus Desktop** app to end users using Jabra personal devices. In the **Jabra Plus Management** platform, you can switch this **OFF** in the default firmware policy in the **Standard Configuration**, disabling firmware management in **Jabra Plus Management** across the board.

Tip

When you want to update the firmware of a Jabra meeting room or personal device model in their respective inventory, you can create a firmware policy that includes an exception for firmware in the **Standard Configuration** or assign a firmware policy to a specific room or device group.

For procedures, see the [modifying & setting the firmware policy for specific Jabra device models](#) or [modifying & setting a firmware policy for a specific room or device group](#).

Although there may be a firmware policy in place for the organization's Jabra personal and meeting room devices, the following requirements must be met before firmware updates can begin:

- The Jabra device must not be in an active call
- Your organization has a weekday and time set in the [scheduled device updates for meeting room devices](#)
- If using a wireless Jabra personal device, the battery must be charged at over 30 percent

During the firmware update, end users must keep their Jabra personal device connected and not adjust any settings until the firmware update process is complete.

If you or end users experience any issues while updating firmware, see the [Recovering your Jabra personal device after a failed firmware update](#) topic or [Troubleshooting](#).

To enable or disable firmware management for meeting room or personal devices:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**
 - For personal devices, click **Personal devices > Configurations**
2. On the **Room configurations** page, click the **Standard Room** pane
 - For personal devices, click the **Standard Configuration** pane
3. On the **Standard Room** page, in the **Firmware Policy** tab, in the **Update devices with Jabra Plus Management** pane, you can toggle the switch **ON**, to enable firmware management within the platform. When you switch it **OFF**, you manage firmware through a third-party service provider
4. In the **Always keep devices updated** pane, you can toggle the switch **ON** to always use the latest firmware for all Jabra meeting room devices in the **room inventory**. When you switch it **OFF**, all Jabra meeting room devices continue using their current firmware version
 - For personal devices, in the **Firmware Policy** tab, in the **Update devices with Jabra Plus Management** pane, you can toggle the switch **OFF** to disable firmware management in **Jabra Plus Management**. When you switch it **OFF**, you cannot manage firmware for Jabra personal devices, and all Jabra personal devices continue using their current firmware version
5. For both personal and meeting room devices, on the bottom ribbon, click **Publish Changes** and confirm

The firmware policy applies when the end user restarts their computer with the connected Jabra personal device. For meeting room devices, the firmware policy changes are applied immediately, but the firmware updates are performed following the [schedule for device updates](#).

Scheduled device updates for meeting room devices

Jabra meeting room devices are an integral part of your organization's meeting rooms, and to keep meeting room devices updated with the latest features, they may require regularly scheduled downtime to implement firmware updates.

As updates are made available by Jabra, a defined maintenance window for your Jabra meeting room devices lets you perform them without interrupting end users.

Scheduled device updates enable you to choose a day of the week at a specific one-hour time interval, whereby the Jabra meeting room devices are temporarily unavailable as their firmware is updated. With a weekly recurring schedule, firmware policy changes made in **room configurations** only take effect during the defined maintenance window.

As a default schedule, all Jabra meeting room devices in your organization's **room inventory** perform available firmware updates between 00:00 and 01:00 (24-hour time format) Monday through Friday.

Note

Currently, for meeting room devices, firmware management is turned **OFF** by default. To switch it **ON**, see the [Enabling or disabling firmware management for Jabra meeting room and personal devices](#) topic.

This default schedule cascades to all [locations](#) and follows the local time zone of the Jabra meeting room device. You can use the default schedule or set a custom weekly schedule for the entire organization.

Note

For Jabra meeting room devices to follow the schedule, they must have a time zone that was set during provisioning.

- **PanaCast U30, PanaCast 40/50/55 VBS, and PanaCast 50 BYOD:** If the time zone was incorrectly set or the meeting room device was moved to a location with a different time zone, you must re-provision the device(s)
- **PanaCast 50 RS:** To set the correct time zone, an admin user must change the Windows® settings for the time zone on the meeting room computer/ThinkSmart™ Core, included in the bundle

Firmware updates take place when following your organization's [firmware policy](#), which governs whether you can update the firmware of Jabra meeting room devices and keep them regularly updated to the latest firmware version.

Unless you have a defined schedule for when updates can be installed, end users may be interrupted during their online meetings. This is due to meeting room devices having to reboot to have the updates applied.

Therefore, updating the firmware of meeting room devices only occurs during the time previously set in the maintenance schedule. If you experience any issues while updating your firmware, see the [Troubleshooting](#) section.

Defining a custom schedule for meeting room device firmware updates

Defining and setting a custom schedule for device firmware updates ensures that Jabra meeting room device downtime in your entire organization only occurs during non-office hours.

Scheduled device updates

Schedule when devices can be updated with new firmware.

Select time range

12:00 AM - 1:00 AM

Local time of the meeting room

Repeats on

S M T W T F S

Cancel Apply

This is based on the local time zone of the device's physical location, therefore minimizing potential interruptions for end users.

Note

Be aware that the custom schedule that you defined and set overwrites the default schedule for all Jabra meeting room device updates in the organization.

To do this:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the left-hand **Locations** bar, at the top of the list, click the action menu (three-dot menu) next to the name of the organization, and click **Scheduled device updates**
3. In the **Scheduled device updates** dialog, on the *Select time range* drop-down menu, choose a timeframe
4. In the **Scheduled device updates** dialog, in the **Repeats on** section, check or click to select at least one weekday, for example, **M** for Monday, **S** for Saturday and so on
 - a. To uncheck, click on the first letter of the weekday, for example, **F** for Friday
5. To save click **Apply**

Viewing the schedule for meeting room device updates

All Jabra meeting room devices in your organization follow an automated schedule that recurs on a weekly basis, on specific days in a specific one-hour timeframe. On the platform, you can view the schedule for updates that apply to your entire organization.

To view the schedule for device updates in the room:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** page, to view the schedule for device updates, on the list of rooms, click the relevant room name
3. On the **Room** page, on the **Details** tab, on the **Date and time** pane, you can see the **Scheduled Device Updates** timeframe

Modifying & setting the firmware policy for specific Jabra device models

You can edit the **Standard Configuration** and set exceptions for managing firmware for specific Jabra meeting room and personal device models that apply to all Jabra meeting room devices in the **room inventory** and **device inventory**.

You can also choose a specific firmware version for a Jabra device model variant, with an exception that applies to all Jabra meeting room and personal devices of the model variants specified.

For example, there may be an organization where you would like to apply a specific firmware version to a model range of e.g. Jabra Evolve3 85 personal devices. With this approach, all Jabra Evolve3 85 personal devices in the organization would have the (exception) setting, in this case, a specific firmware version applied automatically.

Note

Be aware that a firmware version may become unsupported by Jabra. See the [firmware management](#) topic for details.

One common exception that can be set is to toggle the switch **Always use latest firmware** switch **ON**, which lets a specific variant of the Jabra meeting room or personal device model routinely update to the latest firmware version from Jabra.

You can also toggle the **Always keep devices updated** switch **OFF**. This means that all the organization's Jabra personal and meeting room devices retain their current firmware version, and end users are *not* prompted to update to the latest firmware when it is made available by Jabra.

When you want to update the firmware of a Jabra meeting room or personal device model in their respective inventory, you can create a custom firmware policy which requires you to assign or set the created firmware policy to a specific room or device group.



- **For meeting room devices**

Important note

Before installing firmware version **6.5.0** or later, on your PanaCast 50 VBS with Microsoft® Teams as the video service provider, you must migrate the affected Jabra meeting room device to Android Open-Source Project (AOSP) and upgrade to the Microsoft® Device Ecosystem Platform (MDEP). The migration ensures that the connection to your current rooms is not severed by a firmware update to version 6.5.0 or later. For migration procedures, read the [Android Migration Guide](#).

To modify the firmware policy and set it for all Jabra meeting room devices of a specific model:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**
2. On the **Room configurations** page, click the **Standard Room** pane
3. On the **Standard Room** page, in the **Firmware Policy** tab, in the **Update devices with Jabra Plus Management** pane, toggle the switch **ON** to enable firmware management for all Jabra meeting room devices in the **room inventory**

Note

When you switch **OFF** the toggle **Update devices with Jabra Plus Management**, you manage firmware through a third-party service provider.

4. In the **Always keep devices updated** pane, keep the toggle switch **OFF**
5. On the bottom ribbon, when you click **Publish** and confirm, all Jabra meeting room devices continue using their current firmware version
6. To select a specific firmware version or to **Always use latest firmware** for a specific Jabra device model, click **Add model** and on the list, select the relevant Jabra meeting room device model

Note

To ensure touchscreen tablet/touch controller compatibility, be aware that the firmware for your PanaCast 40/50/55 VBS video bars is a bundle containing a package of multiple firmware versions.

See the [Firmware bundles and specific firmware versions](#) topic for guidance.

7. On the bottom ribbon, click **Continue**

8. On the **Manage settings** page, in the **Firmware** pane, toggle the switch **Always use latest firmware** or in the *Firmware version* drop-down menu, select the desired firmware version
 - a. If you choose an older firmware than the one you are currently using, in the **Downgrade firmware** dialog, click **Confirm**
9. If instead you toggled the **Always use latest firmware** switch, to apply the changes, on the bottom ribbon, click **Publish** and in the **Publish model settings** dialog, click **Publish** again to confirm

After you click **Publish**, the custom firmware policy is applied, and any pending firmware updates are performed based on the [schedule for device updates](#).

- **For personal devices**

To modify the firmware policy and set it for all Jabra personal devices of a specific model:

1. On the left-hand navigation bar, click **Personal devices > Configurations**
2. On the **Configurations** page, click the **Standard Configuration** pane
3. On the **Standard Configuration** page, in the **Firmware Policy** tab, switch **OFF** the **Always keep devices updated** toggle
4. On the bottom ribbon, click **Publish** and confirm
5. To choose a specific firmware version for a specific Jabra device model, click the **Model Configurations** tab
6. On the top right-hand side of the page, click **Add model** and select the Jabra devices that you want to set exceptions for, and on the bottom ribbon, click **Continue**
7. On the **Manage settings** page, in the **Firmware** pane, toggle the switch **Always use latest firmware**, or in the *Firmware version* drop-down menu, select the desired firmware version
 - a. If you choose an older firmware than the one you are currently using, in the **Downgrade firmware** dialog, click **Confirm**
8. To apply the changes, on the bottom ribbon, click **Publish**, and in the **Publish model settings** dialog, click **Publish** again to confirm

Tip

If you are modifying more than one Jabra device model, click **Next model** until you see the button **Publish**.

For changes to take effect, ensure you restart the computer to which the Jabra personal device is connected. The changes are applied when the end user logs in to Windows® again.

Modifying & setting a firmware policy for a specific room or device group

For a specific Jabra meeting room device model, an admin user can create a custom firmware policy in a **room configuration** that you created, which lets you set a specific firmware version for a Jabra meeting room device model and then assign it to a room.

You can also assign it to a [room you added](#) with an *empty* room status, so any compatible Jabra meeting room device provisioned to that room immediately follows the custom firmware policy.

For Jabra personal devices, you can create a firmware policy for a **device group** and apply the specific firmware version to all personal device models within the group.

For example, there may be a group of Jabra Evolve3 85 headsets within a device group, and the admin user wants a specific firmware policy to apply to that specific device group. In the case of meeting room devices, the admin user may have a specific firmware policy that was created and would like it to apply to a specific room (with a meeting room device within the room).

Note

Be aware that a firmware version may become unsupported by Jabra. See the [firmware management](#) topic for details.

- **For meeting room devices**

To modify and set a firmware policy for a specific Jabra meeting room device model in a room, you must follow the procedure and then assign the firmware policy to a room.

Note

If you would like to use a specific firmware version with your PanaCast 40/50/55 VBS, be aware that there is an exception. See the [Firmware bundles and specific firmware versions](#) topic.

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**
2. Click the pane with the configuration that you previously created where you would like to set a custom firmware policy
3. In the **Firmware Policy** tab, in the **Update devices using Jabra Plus Management** pane, toggle the switch **ON** and in the **Always keep devices updated** pane, toggle the switch **OFF**
4. Click **Publish changes**, and in the **Publish changes** dialog, and click **Publish again** to confirm
5. On the top right-hand side of the page, click **Add model** and select the Jabra meeting room device model(s), for example, **PanaCast U30**, to which the custom firmware policy applies
6. Click **Continue**
7. On the **Manage settings** page, in the **Firmware** pane, select a specific firmware version or switch **ON** the toggle **Always use latest firmware** for a specific Jabra device model in the relevant configuration
 - a. If you choose an older firmware than the one you are currently using, in the **Downgrade firmware** dialog, click **Confirm**
 - b. If instead you toggled the **Always use latest firmware** switch, at the bottom of the page, on the ribbon, click **Publish** and click **Publish** again to confirm

At this point, for the custom firmware policy to take effect, perform the [assigning a configuration to a device group or a room procedure](#).

- **For personal devices**

To modify & set a firmware policy for a specific Jabra personal device model in a device group:

1. On the left-hand navigation bar, click **Personal devices > Configurations**
2. Click the pane with the relevant configuration where you would like to set a custom firmware policy

3. In the **Firmware Policy** tab, in the **Update devices using Jabra Plus Management** pane, toggle the switch **ON**
4. In the **Always keep devices updated** pane, toggle the switch **OFF**
5. At the bottom of the page, on the ribbon, click **Publish**, and in the **Publish model settings** dialog, click **Publish**
6. On the top right-hand side of the page, click **Add model**
7. Select the Jabra device model(s) to which the custom firmware policy applies, and at the bottom of the page, on the ribbon, click **Continue**
8. On the **Manage settings** page, in the **Firmware** pane, click the drop-down menu and select the firmware you want to use for the relevant configuration or toggle the **Always use latest firmware** switch
 - a. If you choose an older firmware than the one you are currently using, in the **Downgrade firmware** dialog, click **Confirm**
9. At the bottom of the page, on the ribbon, click **Publish** and click **Publish** again to confirm

Next, ensure you assign a firmware policy to a **device group** that you have previously created; otherwise, your firmware policy is not applied.

For the custom firmware policy to take effect, perform the [assigning a configuration to a device group or a room procedure](#).

Firmware recovery for personal devices

See the [Recovering your Jabra personal device after a failed firmware update](#) topic.

7 Software clients & Jabra Plus apps

A software client establishes a connection between an organization's Jabra devices and the platform.

For Jabra personal devices, installing and running a desktop client (i.e.: **Jabra Plus Desktop** app) on a computer is a prerequisite to remote manage Jabra personal devices, also adding them to virtual inventories.

For meeting room devices, there are two different ways of establishing a connection between an organization and the meeting room devices. On the one hand, you can generate and download from the platform, the Jabra Plus room client for the relevant Jabra device type (i.e.: PanaCast 50 RS).

On the other hand, for Jabra meeting room devices with built-in clients (i.e.: PanaCast U30 and PanaCast 40/50/55 VBS) or that require the **Jabra Plus Provisioning** app (i.e.: PanaCast 50 BYOD), you must generate either a *room provisioning code* or *organization provisioning code*, which is also generated from within the platform, and has an expiration date.

Jabra Plus Desktop software client ▼	Jabra Plus room client ▼	Built-in client ▼	Built-in client and using Jabra Plus Provisioning app for provisioning ▼
Jabra personal devices	PanaCast 50 Room System (RS)	PanaCast U30, PanaCast 40/50/55 Video Bar System (VBS) All-in-One & PanaCast 40/50/55 Video Bar System (bar only)	PanaCast 50 —Bring Your Own Device (BYOD)

Important note

You cannot install the **room client** and the **desktop client** (i.e.: **Jabra Plus Desktop** app) on the same computer.

7.1 Jabra personal devices – Jabra Plus Desktop software client

Jabra Plus Desktop is both a software client (desktop client) and an app that connects Jabra personal devices to the platform.

You can generate and download **Jabra Plus Desktop** from within the relevant organization in **Jabra Plus Management**. When you download **Jabra Plus Desktop**, it is recommended to save it with a meaningful name related to the organization. For example, *My Company's desktop application*.

You or an AV Installer must then deploy or distribute this Windows® app to the relevant organization's end users as you best see fit.

Creating and downloading Jabra Plus Desktop

This procedure is a prerequisite to managing Jabra personal devices within the platform. To do this, you must generate or create the software client, which is exclusive to an organization.

To create and download **Jabra Plus Desktop**:

1. On the left-hand navigation bar, click **Personal devices > Desktop clients**
2. Click **Create**
3. In the **Create desktop client** dialog, in the **Name** field, enter a name for your client for example, *Human Resources*, and click **Next**

Tip

When downloading **Jabra Plus Desktop**, ensure you give it a meaningful name. This lets you have a contingency plan in case security or other matters compromise the Jabra personal devices in the grouping.

Therefore, in the case that you must delete **Jabra Plus Desktop** from a relevant organization, you can isolate and stop data transmission from Jabra personal devices in that grouping only and not the entire organization.

4. In the **Download Jabra Plus client** dialog, click **Download**. The **Jabra Plus Desktop** app installation file is downloaded to your default *Downloads* folder associated with your Internet browser.

At this point, you can perform or delegate the installation procedure. For guidance, see the [Device Provisioning & Onboarding Guide](#).

7.2 Jabra meeting room devices – Software clients

To add Jabra meeting room devices to your organization's room inventory in **Jabra Plus Management**, you must follow the relevant provisioning method, i.e.: a Jabra Plus software client for the specific type of Jabra device and its respective setup in a physical meeting room.

Before initiating the provisioning process for Jabra meeting room devices with built-in clients, and depending on the meeting room device, you must [generate a room provisioning or organization provisioning code](#) from within **Jabra Plus Management** and note it down before starting or delegating the relevant procedure described in the [Device Provisioning & Onboarding Guide](#).

The following are the three types of software clients for meeting room devices:

- **Room client** (i.e.: PanaCast 50 RS): You must [create and download the room client](#) (an *.msi file) from Jabra Plus Management. Once you have the Windows®-only file, you or an AV Installer can deploy it on the meeting room computer (or ThinkSmart™ Core) in an MTR, or ZR setup. This is the only software client that supports mass deployment. For deployment options, see the [Device Provisioning & Onboarding Guide](#).
- **Built-in client** (i.e.: PanaCast U30 and PanaCast 40/50/55 VBS): Certain Jabra meeting room devices have built-in software clients with a user interface. Depending on the [provisioning strategy](#) you chose, the admin user or an AV Installer must get either an [organization provisioning code](#) or a [room provisioning code](#). This lets you connect or link the meeting room devices from physical meeting rooms to the platform. During provisioning, you are prompted to choose either MTR, ZR, or BYOD setups.
- **Built-in client with a provisioning app** (i.e.: PanaCast 50): Used exclusively in a BYOD setup, you must use the **Jabra Plus Provisioning** app, along with either the *organization* or *room provisioning code*. This Windows®-only app – available to download via the following [link](#) – lets you or an AV Installer name the device, configure network settings, and set the local time and date.

Creating and downloading a room client

To begin provisioning, you must create and deploy a room client on all meeting room computers connected to your Jabra meeting room device, so they can connect to your organization.

To create and download the room client:

1. On the left-hand navigation bar, click **Meeting rooms > Room clients**
2. Click **Create**
3. In the **Create Jabra Plus room client** dialog, in the **Name** field, enter a name for your client for example, *Meeting room 1 client*, and click **Next**

Tip

You can give the room client a meaningful name, allowing you to have a contingency plan in case security or other matter compromises the Jabra meeting room devices in the relevant grouping.

Therefore, if you must delete a room client from an organization, only the Jabra meeting room devices in that grouping stop sending data to the platform, and not the Jabra meeting room devices in the entire organization.

4. In the **Download Jabra Plus client** dialog, click **Download**. The installation file is downloaded to your default *Downloads* folder associated with your web browser.

At this point, you can perform or delegate the installation procedure. For details, see the [Device Provisioning & Onboarding Guide](#).

Provisioning Codes

Provisioning codes are 12-digit alphanumeric codes used to link or connect Jabra meeting room devices to an organization or room in the **Jabra Plus Management** platform. Admin users can generate two types of provisioning codes based on their [device provisioning strategy](#):

- *Room provisioning code*

Suitable for an organization with an existing [room structure](#), assigned room configuration and/or firmware policies. The *room provisioning code* allows for direct provisioning of compatible Jabra meeting room devices to specific rooms, enabling future peripheral additions like the Jabra Scheduler. After provisioning, the Jabra meeting room devices appear in the **room inventory**, within the existing room structure.

- *Organization provisioning code*

Suitable for organizations without a predetermined room structure. The *organization provisioning code* provisions all Jabra meeting room devices to the **Jabra Plus Management** platform, appearing as an *unassigned room* in the **Locations** bar. Jabra meeting room devices can then be organized into specific rooms/locations, with configuration and/or firmware policies assigned as needed.

Note

Both types of provisioning codes are valid for **14 days** from the day they were generated. During provisioning, if you get a **Code has expired** error message, you must generate a new code before continuing.

Viewing or generating a room or organization provisioning code

A provisioning code is a 12-digit alphanumeric code that connects or links specific Jabra meeting room devices to an organization in the **Jabra Plus Management** platform.

To view or generate an organization provisioning code:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the left-hand **Locations** bar, at the top of the list, click the action menu (three-dot menu) next to the name of your organization, and click **Provisioning code**
3. In the **Provisioning code** dialog, click **Generate code**
4. In the **Provisioning code** dialog, in the *Provisioning code* field, copy or note down the alphanumeric code
 - If you must generate a new code, in the **Provisioning code** dialog, click **Generate a new code**

To view or generate a room provisioning code:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. In the **Meeting room inventory** page, on the left-hand **Locations** bar, in the relevant location, check the checkbox next to the name of the relevant room you would like to generate the room provisioning code for
3. On the bottom ribbon, click **Room provisioning code**
4. In the **Room provisioning code** dialog, click **Generate code**
5. In the **Room provisioning code** dialog, in the *Provisioning code* field, copy or note down the alphanumeric code
 - If you must generate a new code, click **Generate a new code**

At this point, you can perform or delegate the installation procedures, described in the [Device Provisioning & Onboarding Guide](#).

7.3 Deleting Jabra Plus clients

Deleting a Jabra Plus desktop or room client from **Jabra Plus Management** terminates the connection between personal devices or a specific meeting room device (PanaCast 50 Room System) and the platform, effectively stopping the sending or receiving of data; this also means the devices are no longer managed.

You must also uninstall the clients from the relevant computers/meeting room computers.

Note

Built-in Jabra Plus clients (i.e. Jabra PanaCast U30, PanaCast 40/50/55 VBS, and PanaCast 50 BYOD) cannot be removed or deleted from the meeting room devices.

However, you can individually [delete a room](#) or [remove a meeting room device from a room](#), effectively terminating the connection between the meeting room devices and **Jabra Plus Management**.

To delete the Jabra Plus desktop client or room client:

1. On the left-hand navigation bar, click **Personal devices > Desktop clients** or **Meeting rooms > Room clients**
2. Within the relevant **Jabra Plus client** pane you would like to delete, click the action menu (three-dot menu) and click **Delete**
3. In the **Delete Jabra Plus desktop client** or **Delete Jabra Plus room client** dialog, click **Delete**

At this point, the connection to the platform is terminated, and in Windows®, you must uninstall the relevant client using **Add or remove programs**.

8 Appendix for Management Platform

This appendix provides supplementary information to support the main content of the document. It includes detailed technical specifications, procedures, limitations and additional resources that enhance understanding and facilitate implementation.

8.1 Limitations

Jabra Plus Management is currently limited as follows:

- **Personal devices management**
 - End users cannot adjust settings of their Jabra personal device through the **Jabra Plus Desktop** app
 - For personal devices, the following settings are unsupported in all Jabra device models and variants:
 - Sound profile
- **Meeting room devices management**
 - Admin users with restricted access to **Locations** can still modify any **Room configurations**, including any previously created room configurations that were assigned to rooms in restricted locations
 - The PanaCast 40/50/55 Video Bar System (VBS) All-in-one, and the PanaCast 40/50/55 Video Bar System (bar only) do not support the **settings lock** feature.
 - In the **Jabra Plus Management** platform, the following settings for the PanaCast 50 — Bring Your Own Device (BYOD) and PanaCast 50 Room System (RS) are not available:
 - Audio notifications and feedback
 - Room safety capacity notifications (type, timing, and limit)
 - Whiteboard view set up & sharing mode
 - Contrast enhancement
 - Video transition style
 - Preset 1 and 2 – Pan, Tilt, Zoom settings
 - Video flicker
 - Product information
 - For all Jabra meeting room devices, Whiteboard view setup is not yet available
 - The platform does not support the **Room Insights** feature from **Jabra Xpress**

- Automatic migration of room analytics data is not possible between **Jabra Xpress** and **Jabra Plus Management** platform. An admin user (*owner* or *member with edit rights*) can export settings and room information from **Jabra Xpress** to **Jabra Plus Management** platform; however, this must be done manually.

Detailed whitelist domain requirements

Important note

Table 1 outlines the **Jabra Plus Management** platform’s core, images, and analytics related domains. If your organization does *not* permit whitelisting domains with a wildcard (*) prefix, refer to Table 2 for the specific subdomains.

Table 1

	Domain (*= wildcard)	Outbound TCP port(s):	Description
Jabra Plus Management core	<code>https://*.cloud.jabra.com/*</code>	443	Used to access the Jabra Plus Management platform
	<code>wss://*.cloud.jabra.com/*</code>	443	Used by SignalR WebSocket communication layer for responsive UI
	<code>https://*.azure-devices.net/*</code>	443, 5671	Used by Jabra devices, the IoT Hub service facilitates communication with Azure Cloud services
	<code>https://global.azure-devices-provisioning.net/*</code>	443	Needed for device provisioning, regardless of device type (Headset, Android, or Linux)
	<code>https://*.cookiebot.com/*</code>	443	Used for collecting consent. If no consent is given, no data is collected

Jabra Plus images	<code>https://images.ctfassets.net/*</code>	443	Used by the Content Delivery Network (CDN) for Jabra device images
Jabra Plus Management analytics related ¹	<code>https://content.hotjar.io/*</code>	443	Used for heatmaps, screen recordings, and feedback collection.
	<code>https://*.hotjar.com/*</code>	443	Used for heatmaps, screen recordings, and feedback collection.
	<code>https://www.googletagmanager.com/*</code>	443	Used for in-app event statistics collection.
	<code>https://*.google-analytics.com/*</code>	443	
	<code>https://ssl.gstatic.com/*</code>	443	
	<code>https://www.google-analytics.com/*</code>	443	

¹ The following domains and subdomains are used for data gathering at Jabra to improve **Jabra Plus Management** user experience, and general system monitoring. Only anonymized **Jabra Plus Management** usage details are collected, and it does not include personal information. For details, see the data collection topic.

Table 2

If you cannot whitelist parent domains with a wildcard (*) as a prefix, the following table lists the specific subdomains, denoted with a ►).

	Specific subdomain (prefix instead of wildcard)	Outbound TCP port(s):	Description
Jabra Plus Management core	<code>https://*.cloud.jabra.com/*</code>	443	Used to access the Jabra Plus Management platform
	► <code>https://cloud.jabra.com/*</code>	443	Used to access the Jabra Plus Management platform
	► <code>https://signalr.cloud.jabra.com/*</code>	443	Used to establish real-time connections of Jabra devices to the platform and for sending events
	► <code>https://api.cloud.jabra.com/*</code>	443	The main API used by Jabra Plus Management platform software clients
	► <code>https://file.cloud.jabra.com/*</code>	443	Used exclusively to download Jabra Plus Provisioning *.msi files stored in Azure blobs
	► <code>https://content.jabra.com/*</code>	443	Used by the Content Delivery Network (CDN) for translations

	Specific subdomain (prefix instead of wildcard)	Outbound TCP port(s):	Description
	► <code>ntp.jabra.com</code>	123	Used over UDP for time synchronization and <i>Online / Offline</i> status for Jabra meeting room devices
	<code>wss://*.cloud.jabra.com/*</code>	443	Used by SignalR WebSocket communication layer for responsive UI
	► <code>wss://signalr.cloud.jabra.com/*</code>	443	Used by SignalR WebSocket communication
	<code>https://*.azure-devices.net/*</code>	443, 5671	Used by Jabra devices, the IoT Hub service facilitates communication with Azure Cloud services
	► <code>https://jabra-prd-westeu- iothub.azure-devices.net/*</code>	443, 5671	Used by Jabra devices, the IoT Hub service facilitates communication with Azure Cloud services
	<code>https://*.cookiebot.com/*</code>	443	Used for collecting consent. If no consent is

	Specific subdomain (prefix instead of wildcard)	Outbound TCP port(s):	Description
			given, no data is collected
	▶ https://consentcdn.cookiebot.com/ *	443	Used for collecting consent. If no consent is given, no data is collected
	▶ https://consent.cookiebot.com/ *	443	Used for collecting consent. If no consent is given, no data is collected
Jabra Plus Management analytics related	https://*.hotjar.com/ * ▶ https://ws.hotjar.com/ * ▶ https://script.hotjar.com/ * ▶ https://static.hotjar.com/ *	443	Used for heatmaps, screen recordings, and feedback
	https://*.google-analytics.com/ * ▶ https://region1.google-analytics.com/ *	443	Used for in-app event statistics collection.

8.2 Device Management System matrix

The following table informs you of known **Jabra Plus Management** platform compatibility issues with other device management systems and offers recommendations when more than one system is used together at the same time as the platform.

Device Management System	Potential issues	Recommendation
Jabra Xpress	When using both systems (Jabra Plus Management platform and Jabra Xpress) at the same time, duplicate device management can cause a conflict.	Not recommended. Avoid using the Jabra Plus Management platform and Jabra Xpress at the same time. For more information, see the Migration from Jabra Xpress to Jabra Plus Management topic.
Jabra Direct	Using both systems simultaneously can cause device management conflicts, except during initial setup for Jabra meeting room devices or when using older Jabra personal devices. Exception for meeting room devices Setting up <i>Whiteboard view</i> is not supported natively in the Jabra Plus Management platform. Exception for personal devices You can use Jabra Direct or Jabra Xpress to update the firmware of older Jabra personal devices. To check whether your Jabra device is compatible with the Jabra Plus Management platform, see Supported Jabra devices .	Not recommended. Avoid using the Jabra Plus Management platform and Jabra Direct at the same time. Exception for meeting room devices You can still use <i>Whiteboard view</i> in the Jabra Plus Management platform after you set it up in Jabra Direct . After setting up <i>Whiteboard view</i> , you must close, exit, or uninstall Jabra Direct and continue using the platform only. For guidance, see the Jabra meeting room device documentation . Exception for personal devices After updating the firmware using Jabra Direct or Jabra Xpress , ensure you uninstall them.
Lenovo ThinkSmart™ Manager (basic + premium)	When using both systems at the same time, duplicate device management can cause a conflict and settings can be overwritten.	Not recommended. Avoid using the Jabra Plus Management platform and Lenovo ThinkSmart™ Manager at the same time.
Zoom Device Management	Managing device firmware on both device	Choose the Jabra Plus Management platform as the

Device Management System	Potential issues	Recommendation
(firmware management only)	management systems is not recommended.	primary firmware management platform instead of Zoom Device Management. If firmware must be managed using Zoom's Device Management instead of the platform, ensure the firmware policy is disabled on the platform. See the firmware policy chapter for the procedure.
Microsoft Teams Pro Manager Portal	Both device management systems can run at the same time. No known conflicts exist.	Ensure the Jabra Plus Management platform and Microsoft® Teams Pro Manager Portal are set up/configured to avoid conflicts.
Windows Update (firmware management only)	Firmware management can be handled side by side only if one of the two firmware management systems is disabled. Either disable it in the Jabra Plus Management platform or pause Windows Updates.	To keep a fixed firmware version on Jabra meeting room devices, then disable the Always keep devices updated toggle switch in the Jabra Plus Management platform and pause Windows Updates. To do this, see the modifying & setting the firmware policy for specific Jabra device models procedure in the firmware policy chapter.
Crestron XiO Cloud	When using both systems at the same time, duplicate device management can cause a conflict.	Not recommended. Avoid using the Jabra Plus Management platform and XiO Cloud at the same time.

Note

If the organization has Jabra meeting room devices, an *owner* or *member with edit rights* (for meeting rooms) must choose whether to manage firmware through Windows Update or through the **Jabra Plus Management** platform

8.3 Migrating from Jabra Xpress to Jabra Plus Management

The **Jabra Plus Management** platform does not provide tools for automatic migration of settings and room information from **Jabra Xpress** to the platform. This must be done manually.

Important note

There can only be one instance of a Jabra software client running on one individual computer.

If you are a current user of **Jabra Xpress** and/or **Jabra Direct** client, you can optionally migrate settings and room information to the **Jabra Plus Management** platform. To do so, complete the procedure that follows and perform the migration, and afterwards uninstall **Jabra Xpress**.

Be aware that the software clients in **Jabra Plus Management** were designed for a “*clean install*”, i.e., without other Jabra applications previously installed. Therefore, it is not recommended to use the platform’s software clients simultaneously with other Jabra software or partner applications (e.g.: ThinkSmart™ Manager, Jabra Integration Services, **Jabra Xpress**, or **Jabra Direct** client) **on the same computer**.

To prevent conflicts or unexpected behavior – and only after you perform the optional migration – you must uninstall other Jabra software or partner applications before continuing with provisioning Jabra devices into the platform. After migration, you can uninstall the **Jabra Direct** client and stop using **Jabra Xpress** to manage your Jabra devices.

Gradual migration

To reduce downtime, you can perform a gradual migration, as the **Jabra Xpress** solution (i.e.: **Jabra Xpress**, **Jabra Xpress** Cloud, **Jabra Xpress** Tenant, **Jabra Xpress** Packages) can work in parallel with the **Jabra Plus Management** platform.

However, the **Jabra Direct** client must not be installed on the same computer, where the platform’s software clients are also installed.

To perform the migration, ensure you follow procedures A and B.

A. Copy existing settings

To migrate your settings into the **Jabra Plus Management** platform from **Jabra Xpress**:

1. Launch **Jabra Xpress**
2. On the left-hand navigation bar, click **Devices > Manage**
3. Click on the relevant Jabra device and manually copy the settings using your preferred method. For example, you can copy the settings to a text or spreadsheet. After provisioning your Jabra device to the **Jabra Plus Management** platform, ensure you create a [configuration](#) with the settings from **Jabra Xpress**

At this point, you can continue with the next procedure **Export room information**. If you do not have to do this, ensure you uninstall **Jabra Xpress**.

B. Export room information

In **Jabra Xpress**, the **Room Insights** menu item contains analytics information about meeting room(s), room usage, capacity thresholds, Jabra device usage, and more.

You can export this data as a *.csv file and keep it for backup. To do this:

1. Launch **Jabra Xpress**
2. On the left-hand navigation bar, click **Analytics > Room Insights**
3. On the **Select Time Range** ribbon, on the right-hand side of the screen, click **Export**
4. Enter a name for the file and click **Save**
5. Ensure you uninstall **Jabra Xpress**

8.4 Disabling data collection

Data collection lets you gather end user data such as *Computer username*, *Computer information*, and *Location*, among other information. Data collection is enabled by default when you create an organization. However, you can also disable it if necessary.

Data collection is necessary to identify and manage Jabra devices and meeting rooms. More specifically, when the **Data to be collected** checkboxes are checked, the following information is collected and sent to **Jabra Plus Management**:

- **Computer Username:** The username of the operating system where the software client is running

- **Computer Information:** A set of values showing *Computer name, Operating system name, Operating system version, List of IP addresses, Domain name, Computer manufacturer's name, Computer serial number*
- **Location:** Information about computer location if available from the system. This information needs to be accessible to the software client first

Important note

Your organization may want to disable data collection due to legal concerns or privacy policies.

To disable data collection:

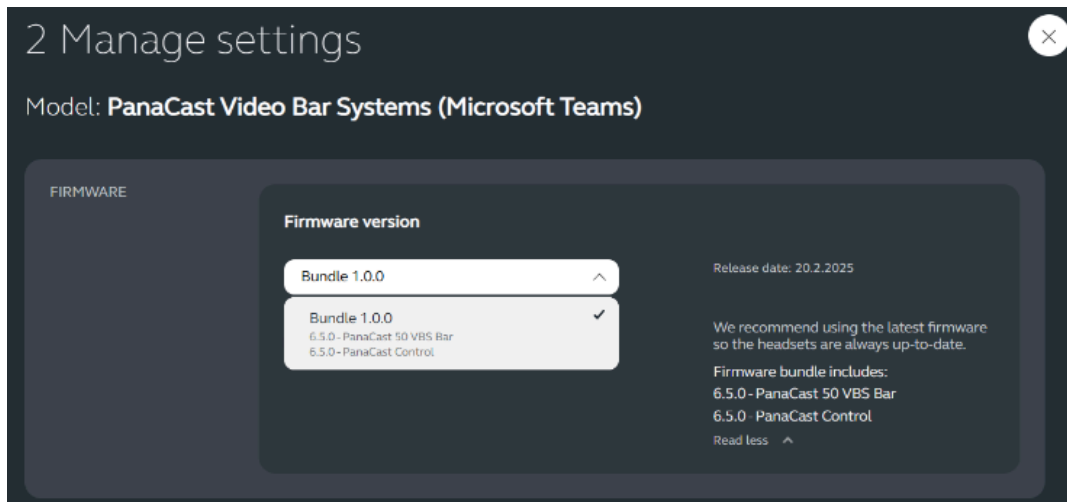
1. On the left-hand navigation bar, click the name of the organization you are currently the owner of or belong to, and then click **Organization settings**
2. On the **Organization settings** page, in the **Data to be collected** section, uncheck the relevant checkboxes, i.e., *Computer information, Location, and Username*
3. To confirm your data collection choices, click **Save**
4. In the **Data collection** dialog, click **OK**

At this point, your Jabra personal and meeting room devices stop sending and collecting data in **Jabra Plus Management**.

8.5 Firmware bundles and specific firmware versions

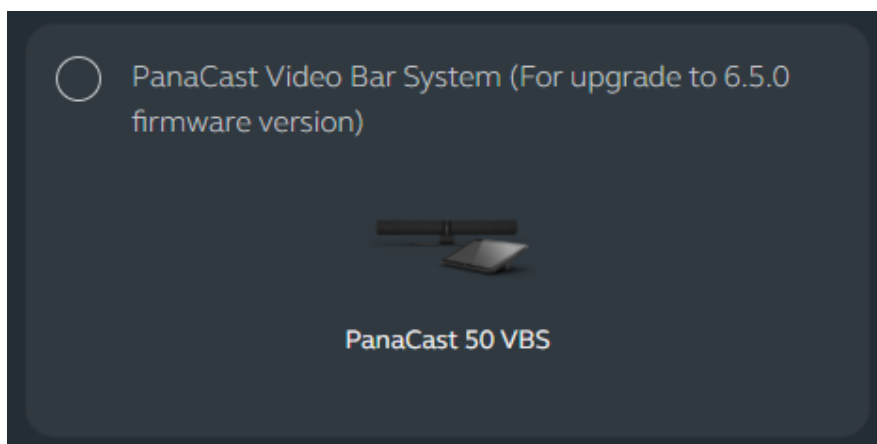
Firmware bundles are exclusive to PanaCast 40, 50, and 55 VBS video bars, and they contain a package of firmware versions that ensure the touchscreen tablet/touch controller can work with the video bar, avoiding incompatibility issues. This is due to the tablet having its own firmware.

For example, **Bundle 1.0.0** includes two firmware: one for the video bar (i.e. **6.5.0 PanaCast 50 VBS bar**) and another for the touchscreen tablet/touch controller (i.e. **6.5.0 PanaCast Control**).



Specific firmware versions for PanaCast 50 VBS

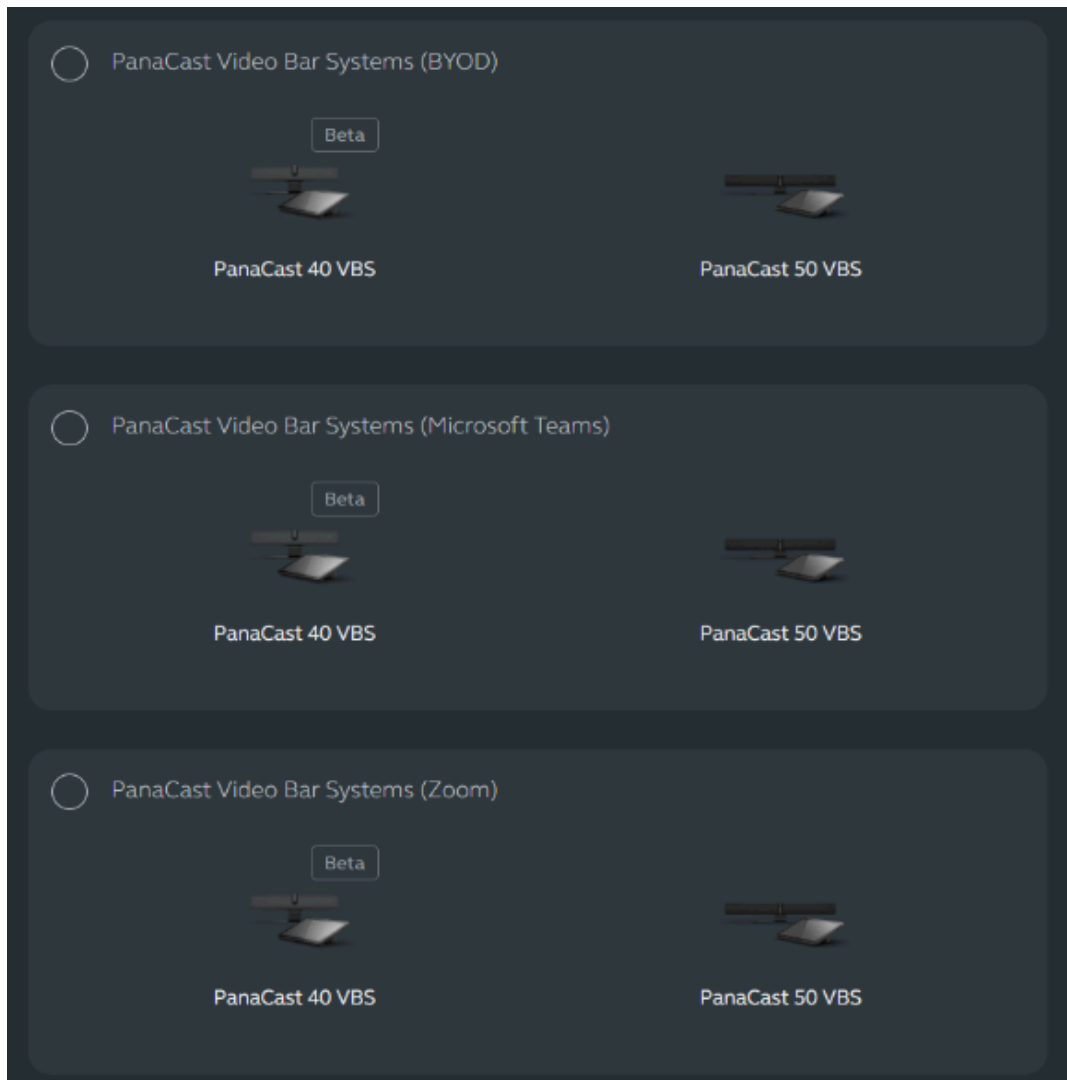
When you create a room configuration from scratch, or set exceptions in the **Standard Room Configuration**, and you want to run an earlier firmware version than **6.5.0**, you must select the old card i.e.: *PanaCast video bar system (Firmware release: February 2025 or older)*



Important note

Before installing firmware version **6.5.0** or later, on your PanaCast 50 VBS with Microsoft® Teams as the video service provider, you must migrate the affected Jabra meeting room device to Android Open-Source Project (AOSP) and upgrade to the Microsoft® Device Ecosystem Platform (MDEP). The migration ensures that the connection to your current rooms is not severed by a firmware update to version 6.5.0 or later. For migration instructions, read the [Android Migration Guide](#).

However, if you have updated the firmware of your PanaCast 50 VBS to version **6.5.0** or later, then you must select the PanaCast 50 VBS option together with the relevant video service provider i.e.: *Microsoft Teams, Zoom* or *BYOD*.



8.6 Duplicating a configuration for personal or meeting room devices

You can also duplicate a configuration or room configuration and assign it to many rooms or **device groups**.

Duplicating a configuration with custom Jabra device model settings, firmware policy, and locked end user settings allows you to create multiple similar configurations/room configurations and make small changes if necessary.

To duplicate a configuration/room configuration:

1. On the left-hand navigation bar, click **Meeting rooms > Room configurations**, or in the case of personal devices, click **Devices > Configurations**
2. On the **Room configurations/Configurations** page, click the pane with the configuration name you would like to duplicate
3. On the configuration page you would like to duplicate, on the top right-hand side of the screen, click the action menu and click **Duplicate configuration**

4. In the **Duplicate configuration** dialog, in the *Configuration name* field, enter a name. Optionally, in the *Description* field, enter a description for the duplicated room configuration/configuration
5. Click **Save Changes**

For your duplicated configuration to take effect, you must [assign a configuration to a device group or a room](#).

8.7 Bulk-assigning a room configuration to many rooms

For a configuration to take effect on specific rooms with Jabra meeting room devices and replace the default **Standard Room Configuration** for the specific rooms, you must change the assigned configuration of the room. When required, you can also select multiple rooms and bulk assign a room configuration that was created.

To bulk-assign a room configuration to many rooms:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** table, check the checkbox for the relevant room name(s)
3. On the bottom ribbon, click **Assign configuration**
4. In the **Change room configuration** dialog, in the drop-down menu, select the configuration name you created, and click **Apply** to confirm.

Now, you have bulk-assigned a Room configuration you created for one or many rooms.

8.8 Rebooting Jabra meeting room devices

The **Jabra Plus Management** platform lets you remotely reboot Jabra meeting room devices. The reboot feature is the first step in troubleshooting any undesired behavior or errors, and can be performed on all Jabra meeting room devices.

In the case of PanaCast 40/50/55 VBS, both the meeting room device and the Jabra PanaCast Control/Touchscreen tablet are simultaneously rebooted.

Important note

Rebooting Jabra devices from within the platform is only available when the Jabra meeting room device appears *Online* (connected) in the [room inventory](#). Also, the Jabra meeting room device must not be in an active meeting or call; otherwise, the **Reboot device** option is unavailable or greyed out.

To reboot a Jabra meeting room device:

1. On the left-hand navigation bar, click **Meeting rooms > Room inventory**
2. On the **Meeting room inventory** page, in your **Locations** tree structure, click the name of your organization
3. On the **Meeting room inventory** table, click the relevant room name
4. On the **Room** page, on the relevant pane that shows the Jabra meeting room device you would like to reboot, click the action menu and click **Reboot device**
5. In the **Reboot device** dialog, click **Confirm**

8.9 Pairing your Jabra personal devices to work with Jabra Plus Management

For **Jabra Plus Desktop** to work with your wireless Jabra personal device and make a connection to the **Jabra Plus Management** platform, you must install the Jabra Link Bluetooth adapter and pair it to your Jabra personal device.

Note

Be aware that for wired Jabra personal devices (e.g.: Jabra Evolve2 50) you do *not* have to perform the procedure that follows, as **Jabra Plus Desktop** automatically detects wired personal devices.

As a prerequisite, ensure you have first installed **Jabra Plus Desktop** on the end user's computer where you are going to pair your personal device and adapter to.

To pair your Jabra Link Bluetooth adapter (i.e.: Jabra Link 370, 380, 390 and variants) and Jabra personal device (Bluetooth device):

1. Insert the Jabra Link Bluetooth adapter into a USB port on your computer and ensure the Jabra personal device is switched **ON** and within range
2. Put your Jabra personal device in pairing mode. (See the Jabra personal device's manual for instructions on how to do this)

3. On your Windows system tray, right-click the **Jabra Plus Desktop** icon and click **Pairing**

When the **Jabra Plus Desktop** app detects your Jabra Link Bluetooth adapter, it searches for your Jabra personal device. When detected, in the **Available devices** dialog, click the Jabra personal device you would like to pair. When pairing is successful, you see a **Device connected** message.

The Jabra personal device is now paired and can be managed remotely in **Jabra Plus Management**.

8.10 Recovering your Jabra personal device after a failed firmware update

In **Jabra Plus Desktop**, if your firmware update fails, it is interrupted or did not complete, the end user is prompted to recover their Jabra personal device.

During the recovery process, the app retries installing the previously failed firmware update.

Note

The following procedure applies only to cabled or wired Jabra personal devices. Jabra wireless or Bluetooth personal devices do not need to be recovered.

To perform firmware recovery on wired or cabled Jabra personal device(s):

1. If your firmware update fails, a notification informs you, and you can begin the recovery process. In the **Something went wrong** dialog, click **Recover device**

Note

You may be asked to unplug or undock all other Jabra devices to start the recovery.

2. **Recovery in progress** dialog shows the duration of the recovery. When it is finished, in the **Recovery complete** dialog, click **OK**

The recovery is now completed. The **Jabra Plus Desktop** app checks again whether your Jabra personal device requires a firmware update. Click **OK** to finish.

8.11 Changing the Jabra Plus Management platform interface language

Any admin user can change the interface language on the platform. Be aware that changing the interface language only affects the **Jabra Plus** account of the admin user.

To do this:

1. On the left-hand navigation bar, click your profile name (user icon)
2. Click **Personal details**
3. In the **Language preference** pane, in the **Language** drop-down menu, choose a language, and click **Save changes**

The selected language is applied in your browser, and platform menu items are immediately displayed in the chosen language.

9 Troubleshooting

Problem	Solution
<i>I have modified my Jabra account profile information, but the changes are not reflected on the Jabra Plus Management platform. Note If you have enabled SSO in your organization, you cannot perform this procedure.</i>	1. On the left-hand navigation bar, click your profile name (user icon) 2. Click Personal details 3. On the Personal details page, click the Edit profile button. You are now taken to an external webpage 4. In the <i>Account</i> tab, under Display name , click Edit 5. In the provided field, enter the new display name and click Save Now, you can close the web browser and return to the platform. Ensure you log out of the platform and log back in to see the reflected changes to your display name in the Profile > Personal details page. 6. At this point, on the Personal details page, click the Sync profile button. You will get a notification that your profile on Jabra.com has been synchronized with the platform.
<i>I created and installed a software client, but my Jabra device (Meeting room or Personal device) does not appear in the room inventory or device inventory.</i>	- If the Jabra meeting room or personal device is not visible in the relevant inventory, the end user must restart the computer that the Jabra device is connected to.
<i>I tried to update the firmware of my Jabra meeting room device; however, the process stopped during the update, and I cannot continue updating it.</i>	- PanaCast 50 RS: If the firmware update fails, ensure you reboot the Jabra meeting room device. The firmware update resumes automatically, in the context of scheduled device updates . - PanaCast 50 BYOD: Ensure you unplug the Jabra meeting room device from the power supply/outlet and plug it back in. You can now retry the firmware installation. - PanaCast 40/50/55 VBS: See the error message displayed in the PanaCast Control/Touchscreen tablet. Restart/reboot the Jabra meeting room device and retry the firmware update. Important note For instructions on how to reboot, ensure you read the relevant Jabra meeting room device documentation .
<i>As an end user, I tried to update the</i>	- You must perform a firmware recovery. See the Recovering your Jabra personal device after a failed

Problem	Solution
<i>firmware of my Jabra personal device, but the process was interrupted or did not complete, and my device does not work, or the firmware was not installed.</i>	firmware update topic. Be aware that this procedure only applies to cabled or wired Jabra personal devices.
<i>When I want to perform a procedure, some of the menus appear greyed out or unavailable.</i>	The admin user performing the procedure may not have the correct permission to do so. See the Roles and permissions chapter.
<i>I tried to update the firmware of certain Jabra personal devices on the platform, however, I see a message “Firmware updates are not supported in Jabra Plus Management, use Jabra Direct or Jabra Xpress to update the device when required”, how can I update the firmware of my Jabra personal device(s)?</i>	- Jabra personal devices with older hardware must be firmware updated using Jabra Direct or Jabra Xpress . Ensure that you first update the firmware using Jabra Direct or Jabra Xpress , and after the update is completed, you must uninstall Jabra Direct (or stop using Jabra Xpress) and continue using the Jabra Plus Desktop . For the list of Jabra personal devices that may require a firmware update using Jabra Direct or Jabra Xpress , see the Supported Jabra devices list . Be aware that some of the settings of your older personal device(s) may not be available on the platform.
<i>There is a Configuration warning message in a (room) configuration (or configuration for personal devices)</i>	- When a previously selected firmware version in a configuration becomes unsupported, subsequent Jabra devices added to the respective inventories keep their existing firmware and cannot update to the unsupported version. - To remove the exclamation mark (!) and the Configuration warning message, you must select a different firmware version and edit the

Problem	Solution
<i>that I created. How can I address the warning? I also see an exclamation mark (!) on some Jabra devices in my device inventory or room inventory.</i>	firmware policy. To do this, see the procedure Modifying & setting the firmware policy for specific Jabra device models or if you have configurations assigned to a specific room or Jabra personal devices in a device group, see the Modifying & setting a firmware policy for a specific room or device group procedure.
<i>I successfully provisioned Jabra devices to the Jabra Plus Management platform, but the connection status shows Offline. How do I get Jabra devices to appear Online (Connected) in my device inventory or room inventory ?</i>	- A device that is listed in an inventory but shows as <i>Offline</i> has successfully established an initial connection to the platform. However, it cannot establish or maintain a persistent connection to cloud services. This ongoing connection relies on WebSocket technology over HTTPS. - Confirm that the Jabra device, or the computer it is connected to, has internet access - Verify that the corporate firewall allows outbound HTTPS traffic on TCP port 443 to all required Jabra Plus endpoints listed in the Detailed whitelist domain requirements section - Ensure that your network infrastructure permits WebSocket connections to *.azure-devices.net. Proxies or security appliances must allow the HTTP Upgrade handshake to this endpoint and must not terminate long-lived connections prematurely. - If your organization performs TLS inspection (SSL decryption), verify that *.azure-devices.net is excluded, as inspection may interfere with the WebSocket connection Important note *In the case that your organization uses a proxy server or a specific NTP server URL, verify that the proxy settings are correct and that Jabra Plus traffic is allowed. For certain Jabra meeting room devices that use the Jabra Plus Provisioning app (i.e., PanaCast 50 BYOD), you must configure the network and proxy server settings during provisioning. For the procedure, see the Device Provisioning & Onboarding Guide. For other Jabra meeting room devices (i.e., PanaCast U30 and PanaCast 40/50/55 VBS), ensure that you read the relevant Jabra meeting room device documentation.

If you require further assistance, would like to get in touch with Jabra, or consult other documents, ensure you visit the [Jabra Plus support](#) page.

