# Plantronics Manager Pro

User Guide, v 3.11.1

# Contents

# Setup

After you establish your Plantronics Manager Pro account, you must download and deploy Plantronics Hub, the client software, to your users. Plantronics Hub is the key to all activities.

Here are the required steps for setup.

1. Request and establish an account.
2. Download and deploy Plantronics Hub.

## Request and establish an account

1. Contact your Plantronics reseller to request an account.
When the tenant setup is completed by Plantronics, you will receive an email with account information.
**IMPORTANT** *During this process, the information provided establishes the primary contact administrator. This can be changed later, as well as adding additional administrators, by going to* ***Admin*** *>* ***Accounts*** *>* ***Administrators****. For more information, see* Manage administrators
2. Login to the URL provided in the email to establish your account.

## Configure your environment

Service operation requires secure access to the following URLs for the Plantronics Hub client and tenant administration.

It is recommended that you whitelist the URLs provided (based on region).

**US**

https://<tenant>.plantronicsmanager.com

https://df84x76lg9aky.cloudfront.net

https://downloads.plantronicsmanager.com

https://d12903byg7ot3n.cloudfront.net

https://duk8mtqrgwh9y.cloudfront.net

https://help.plantronicsmanager.com

https://auth.plantronicsmanager.com

https://api.plantronicsmanager.com

https://system-api.plantronicsmanager.com

https://reports.plantronicsmanager.com

https://clientregistration.plantronicsmanager.com

**Europe**

https://<tenant>.plantronicsmanager-eu.com

https://df84x76lg9aky.cloudfront.net

https://downloads.plantronicsmanager.com

https://d12903byg7ot3n.cloudfront.net

https://d2x2ehj0htq0t6.cloudfront.net

https://help.plantronicsmanager.com

https://auth.plantronicsmanager-eu.com

https://api.plantronicsmanager-eu.com

https://system-api.plantronicsmanager-eu.com

https://reports.plantronicsmanager-eu.com

https://clientregistration.plantronicsmanager-eu.com

**Asia**

https://<tenant>.plantronicsmanager-ap.com

https://df84x76lg9aky.cloudfront.net

https://downloads.plantronicsmanager.com

https://d12903byg7ot3n.cloudfront.net

https://d1k6f42hn7at4y.cloudfront.net

https://help.plantronicsmanager.com

https://auth.plantronicsmanager-ap.com

https://api.plantronicsmanager-ap.com

https://system-api.plantronicsmanager-ap.com

https://reports.plantronicsmanager-ap.com

https://clientregistration.plantronicsmanager-ap.com

**Australia**

https://<tenant>.plantronicsmanager-au.com

https://df84x76lg9aky.cloudfront.net

https://downloads.plantronicsmanager.com

https://d12903byg7ot3n.cloudfront.net

https://d1utxqry92nfl9.cloudfront.net

https://help.plantronicsmanager.com

https://auth.plantronicsmanager-au.com

https://api.plantronicsmanager-au.com

https://system-api.plantronicsmanager-au.com

https://reports.plantronicsmanager-au.com

https://clientregistration.plantronicsmanager-au.com

*URL descriptions*

- **https://<tenant>.plantronicsmanager-[region].com** tenant URL
- **https://df84x76lg9aky.cloudfront.net** used to download firmware updates
- **https://downloads.plantronicsmanager.com** used to download firmware updates
- **https://d12903byg7ot3n.cloudfront.net** used to download custom MSI installers
- **https://help.plantronicsmanager.com** used to view help documentation
- **https://auth.plantronicsmanager-[region].com** used to authenticate Hub clients
- **https://api.plantronicsmanager-[region].com** used for events and Hub client data transmission
- **https://system-api.plantronicsmanager-[region].com** used for older client authentication and client data transmission
- **https://reports.plantronicsmanager-[region].com** used to access reports
- **https://clientregistration.plantronicsmanager-[region].com** used to register mobile clients
- **https://duk8mtqrgwh9y.cloudfront.net** used for mobile devices to download FW in NA
- **https://d2x2ehj0htq0t6.cloudfront.net** used for mobile devices to download FW in EU
- **https://d1k6f42hn7at4y.cloudfront.net** used for mobile devices to download FW in AP
- **https://d1utxqry92nfl9.cloudfront.net** used for mobile devices to download FW in AU

## Download and deploy Plantronics Hub for Windows

Plantronics Hub, the client software, must be installed on your user's systems to populate your tenant.

1. Ensure that previous versions of Plantronics software such as Plantronics Spokes or PURE have been uninstalled.
2. With the Plantronics Manager Pro open, go to **Admin** > **Plantronics Hub** > **Installing Client | WIN**.
3. Following the instructions, generate your tenant-specific installer. This may take a few minutes.
   **IMPORTANT** *The installer generates an MSI using the latest version of Plantronics Hub.*

   **NOTE** *If you don't know if your user requires a 32- or 64-bit .msi file, there is an executable version of the Plantronics Hub installation file that incorporates both the 32- and 64-bit .msi files. See* Troubleshooting > Installation.
4. Download the installer with the link provided or alternatively, check **Home** > **Notifications** for an alert informing you that the package is ready.
5. Deploy Plantronics Hub manually or with a software distribution system.
   - To deploy Plantronics Hub without a desktop shortcut, add the additional parameter **HIDEDESKTOPSHORTCUT=1** in the command line. Below is an example.

     ```
     msiexec /i PlantronicsHubInstaller_x32.msi HIDEDESKTOPSHORTCUT=1
     ```

### Language support (Windows only)

Plantronics Hub can be installed in over 20 different languages. It is installed in the language specified in the System Preferences "Language and Text" settings of the computer on which Plantronics Hub is being installed when the locale is supported. When the locale is not supported, Plantronics Hub is installed in English.

### Run Plantronics Hub in a different locale

To specify a different locale for Plantronics Hub, use the "-lang" option with one of the supported locales. The supported locales are listed in the directory C:\Program Files (x86)\Plantronics \Spokes3G\locales on Windows.

From a Windows command line, follow these steps:

1. Change to the directory where the Plantronics Hub application is hosted. For example, use this command: cd C:\Program Files (x86)\Plantronics\Spokes3G\
2. Start the Plantronics Hub executable with the -language=<locale> option. For example: PLTHub.exe -language=fr-FR (for French). Plantronics Hub opens in the specified locale language.

### Run the Plantronics Hub installer in a different language

1. To specify a language other than the default, en_US, when installing Plantronics Hub, use the "/lang" option with the Microsoft-defined locale identifier like this:
   PlantronicsHubInstaller.exe /lang <locale_id_dec>
   For example, to install Plantronics Hub in Spanish - Mexico, run the installer like this:
   PlantronicsHubInstaller.exe /lang 2058
   **NOTE** *Options for <locale_id_dec> are documented at* msdn.microsoft.com/en-us/goglobal/bb964664.aspx*. Use the decimal values, not the hexadecimal. Convert hexadecimal to decimal here:* https://www.binaryhexconverter.com/hex-to-decimal-converter.
2. If you want to run Hub in a different language other than OS, you can create a batch scripting and force it to run during system boot-up (as a part of login scripting)
   **IMPORTANT** *The language needs to be part of the 20 languages that Plantronics supports. Specify the language details in bold below.*

```
@echo off

taskkill /F /IM PLTHub.exe

cls

cd C:\Program Files (x86)\Plantronics\Spokes3G\

START PLTHub.exe -language=es-ES -m

Exit
```

### Adding Plantronics Hub to a system image

The Plantronics Hub client should NOT be installed or captured in a *base* image. Instead, install Plantronics Hub during the imaging task sequence or a post-imaging step after the base image has been applied to the system.

Plantronics Hub for Windows installs a unique identifier (registry key) called the SystemID that prevents users from being duplicated when Plantronics Hub is removed and then reinstalled on the same system. If Plantronics Hub is installed on a base image, this SystemID will be duplicated on each system. In this case, all users are associated to the same SystemID causing inventory and insights to no longer be accurate.

## Download and deploy Plantronics Hub for Mac

Plantronics Hub, the client software, must be installed on your user's systems to populate your tenant.

1. Ensure that previous versions of Plantronics software such as Plantronics Spokes or PURE have been uninstalled.
2. With the Plantronics Manager Pro open, go to **Admin** > **Plantronics Hub** > **Installing Client** | **MAC**.
3. Download the Mac.dmg by clicking on the button.
4. Copy the full path of the directory for the location of the .dmg.
5. To generate your tenant-specific installer script, click the "Create Installer Script" button.
   **IMPORTANT** *The installer generates a script using the latest version of Plantronics Hub.*
6. Paste the .dmg directory path into the script generator.

7 Copy, paste and run the generated installer script from Terminal (**Go** > **Utilities** > **Terminal**). This establishes the relationship between Plantronics Hub and your tenant.

8 Deploy Plantronics Hub manually or with a software distribution system.

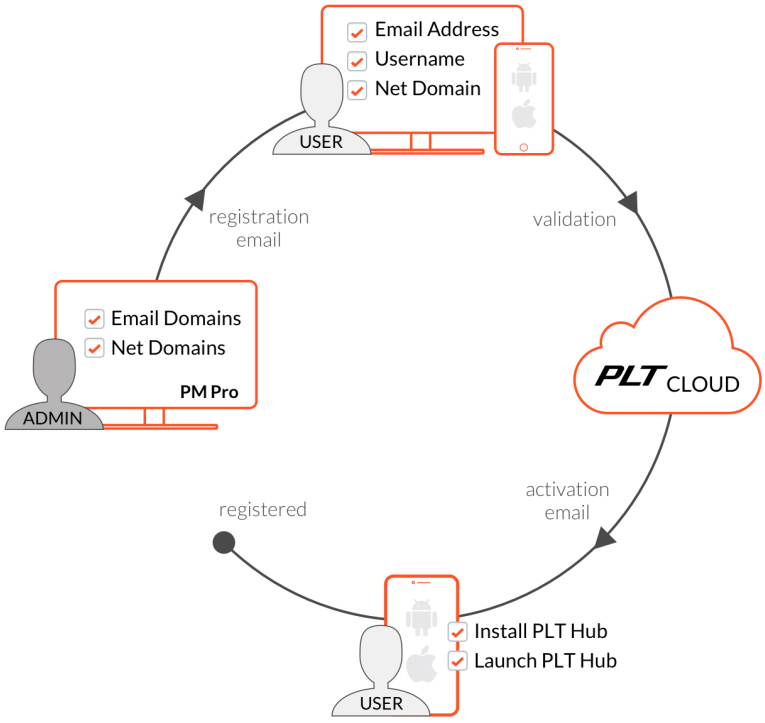
## Download and deploy Plantronics Hub for mobile devices

You can integrate Plantronics Hub for Android/iOS users into your enterprise tenant for Plantronics Manager Pro.

**Supported devices** Mobile phone inventory and firmware/settings management is supported for:

- Voyager 3200 UC
- Voyager 6200 UC
- Voyager 5200 UC
- Voyager 8200 UC
- Voyager Focus UC (firmware cannot be updated on mobile platform)

### Mobile registration workflow




### PMP configuration for mobile

Go to **Admin** > **Plantronics Hub** > **Integrating Mobile Hosts**. Populate the fields and copy and paste the registration URL into a registration email.

- **Valid Domains** Populate the domain information. Plantronics Hub attempts to discover and auto-populate this field (assuming Plantronics clients have been deployed). The domains entered appear in a drop-down box for user selection during the user registration process.
- **Valid Email Domains** Populate the valid email domains. This is used to validate the email address entered by users during the user registration process.

- **Copy the registration URL** and paste this link into an email to your users. Example email content is available by selecting the Email Template link in the UI. Send the email using your own email client, outside of the Plantronics Manager Pro environment. The registration URL does not expire and it can be revoked. To revoke the registration URL for all mobile users, go to **ADMIN** > **Plantronics Hub** > **Integrating Mobile Hosts** and select the "Revoke URL" button. For a single user, go to **Inventory** > **Hosts**, select the user and click "Revoke mobile access.

**Mobile user registration process**

1. Selecting the registration URL, users will provide *their* username and email and select a corporate domain. The email domain will be validated against the IT provided Valid Email Domains.
2. Upon successful validation, Plantronics Manager Pro auto-generates a second email to the user. Please note that the activation link included in this email expires 5 hours after generation. The user is required to complete the steps on their mobile device:
   - Download latest version of Plantronics Hub
   - Launch Plantronics Hub, accepting all prompts and permissions
   - Click on the activation link
3. Plantronics Hub for Android/iOS connects to your tenant and creates an account if one does not already exist. Existing accounts will be identified by Plantronics Manager Pro and the mobile device is added as a new host in the user's profile.

## Download and deploy Plantronics Hub for VDI environments

For Plantronics Hub installation support for Virtual Desktop Infrastructure (VDI) environments, visit this link: https://www.plantronics.com/content/dam/plantronics/documents-and-guides/en/user-guides/Plantronics_Support_for_VDI.pdf.

# Create groups

The purpose of defining user groups is to make it easy to deploy firmware/software/settings updates to the appropriate users in your organization. In Plantronics Manager Pro, groups are created manually or based on LDAP group queries that you define. Each installation of Plantronics Hub polls the deployment server on a regular basis and compares with the group definitions to determine to which groups a user is assigned.

The LDAP group membership can be seen in Plantronics Hub by going to **Help** > **Support** > **Troubleshooting Assistance**.

## Check device inventory

The "Company Snapshot" on the Home page is a quick way to view devices.

When you first open Plantronics Manager Pro, the Home page displays. At the bottom of this page is a snapshot of devices registered by users in your organization. When a user starts Plantronics Hub and plugs in a device, that device is added to the others and the data in this section will be updated to reflect the new inventory.

For a more in-depth device inventory report, see Reports.

## Configure your LDAP server

You can leave the LDAP server information blank, if your LDAP server is auto-discoverable, uses standard ports and doesn't use SSL. This is because Plantronics Hub will auto-discover your LDAP server and query the nearest domain controller. You only need to specify fields in LDAP server configuration that are not standard.

1. To configure your LDAP server, go to **ADMIN** > **Plantronics Hub** > **LDAP** and click on "Edit settings" on the top right of the screen.
2. **If your LDAP server is not auto-discoverable** Enter your LDAP server address. For example, *xyz.yourcompany.com.*
3. **If your LDAP server does not use standard ports** Enter your LDAP server port. Typically LDAP servers run on port 389 for regular connections and on port 636 for secure connections.
4. Select the type of Directory Service you are using.
   **NOTE** *"Active Directory" and "Open LDAP" queries use different names for some fields.*
5. Enter your LDAP version.
6. **If your LDAP server uses SSL** Enable a secure connection in the "SSL" field.
7. Click SAVE. Changes are deployed when the next polling cycle occurs.

## Create an LDAP Group

Create a group based on criteria already defined in your LDAP database. LDAP-created groups will automatically include users that satisfy the stated LDAP Query. Clients are updated the next time there is a client poll or when they stop and restart Plantronics Hub. Both of these events authenticate the user. At that point, the Inventory > Users listing will be updated to reflect the group with the highest priority to which the user belongs.

1. From the Inventory > Groups > All Groups page, click "Create Group."
2. To create an LDAP group, select "LDAP," and then click the "Create Group" button.
3. Enter "Group Details."
   Here are a few examples you might wish to use as a basis for creating your LDAP queries. Check your company's LDAP documentation for help writing LDAP queries.
   **TIP** *Plantronics Hub for iOS/Android users must have Plantronics Hub for desktop installed in order to be associated with an LDAP group.*

1. For Open LDAP:

```
Group: Users in the Sales Force: (&(objectCategory=person)(objectClass- s=inetOrgPerson)(uid=
$user$)(department=*sales*))
Group: Users in Human Resources: (&(objectCategory=person)(objectClass- s=inetOrgPerson)(uid=
```

$user$)|(department=*hr*) (department=*Human Resources*))
Group: Users Located in Building 345, Santa Cruz, CA: (&(objectCategory=person)(objectClass-s=inetOrgPerson)(uid=$user$)(physicaldeliveryofficename=US-SantaCruz) (streetaddress=345*))
Group: Users in "Sales" located in office "US-SantaCruz": (&(objectCategory=person)(objectClass-s=inetOrgPerson)(uid=$user$)(department=*sales*) (physicaldeliveryofficename=US-SantaCruz))
Group: Users either in "Sales" or located in Santa Cruz: (&(objectCategory=person)(objectClass-s=inetOrgPerson)(uid=$user$)(|(department=*sales*)(physicaldeliveryofficename=US-SantaCruz)))

2 For Active Directory:

Group: Users in the Sales Department: (&(objectCategory=person)(objectClass=user)(sAMAccountName=$user$)(memberof=CN=Sales, OU=Groups, DC=domain, DC=com))
Group: Users in "Sales" located in office "US-SantaCruz": (&(objectCategory=person)(objectClass=user)(sAMAccountName=$user$)(memberOf=CN=Sales, OU=Groups, OU=US-SantaCruz, OU=Americas, DC=domain, DC=com))

**IMPORTANT** *The (sAMAccountName=$user$) field is required for all LDAP queries. Plantronics Hub replaces this pattern with the user's account name and checks to determine if the user belongs to a particular group.*

4 Click the "Save" button to create the group.
No further action is needed to add members to the group. When Plantronics Hub applications poll for updates, users will be added to the group if they meet the criteria.

5 To confirm that the correct users are added to the group after the polling cycle has completed, select the group from the Inventory > Groups list and view "Group Membership."

## Create a manual group

Create groups of users that are not defined in your LDAP database.

1 From the **Inventory** > **Groups** > **All Groups** page, click "Create Group."
2 To create a manually-defined group, select "Manual," and then click the "Create Group" button.
3 Enter and save "Group Details."
4 Click "All Groups" or **Inventory** > **Groups** to go to the **Inventory** > **Groups** > **All Groups** page.
A listing of all groups displays. Select the manual group you just created to add members to that group.
5 Click the "Add User" button.
The "Assign to Group" dialog displays with a listing of all users in your organization.
6 Select users by clicking the checkbox beside their name.
To narrow the list, you can use the "Search" feature to search for users based on their name, status or priority group.
7 Click the "Assign to Group" button to select members for this group.

## Manage user accounts

### Create shared user accounts

Shared user accounts help you manage environments where multiple users sign into a single, shared account.

By adding one or more shared accounts for your tenant, individual users signing in with a single, shared username will be identified as a combination of the username + hostname. This permits management of settings/updates and accurate data collection on a per user basis.

To create an individual user account when an account login is shared with multiple users, go to **Plantronics Hub** > **Shared User Accounts** and click "Add Account."
The computer name is appended to the account name to allow Plantronics Manager Pro to accurately report and deploy updates.

### Exclude user accounts

Use excluded accounts to have Plantronics Manager Pro ignore selected network accounts for all related activities and data collection.This feature is intended to support Virtual Desktop (VDI)

environments as well as system management accounts that you may wish to exclude from Plantronics Manager Pro management.

To exclude an account, go to **Plantronics Hub** > **Exclude Account** and click "Add Account."

### Revoke mobile access

Mobile access can be revoked for user/hosts that are no longer valid.

To revoke mobile access for a single user, go to **Inventory** > **Hosts**. Click on the desired host and click "Revoke mobile access."
All tenant connection information will be deleted and Plantronics Hub for Android/iOS will revert to a consumer version of Plantronics Hub.

# Manage firmware and software

Device firmware, software and updates are configured with firmware and software policies.

## Configure FW/SW policies

A firmware or software policy:

- applies to all users, until customized for a specific group
- is active once it is enabled and saved (it is initiated the next time the polling cycle occurs)
- can be edited, deleted or copied

### Create a new firmware or software policy

Create a new policy by going to **Policy** > **Firmware/Software** > **Create New Policy** (button in the upper right).

### Copy a firmware or software policy

To copy and modify a policy, go to **Policy** > **Firmware/Software** and hover over the target policy. Click the Copy icon at the far right. Updates to copied policies do not affect the original polices.

### Preconfigure a device

To preconfigure a device that has not been deployed, go to **Policy** > **Firmware/Software** > **Create New Policy** . Unclick the "Show my tenant's devices only" box to choose from devices that are not in your current environment.

### Edit a policy

**To edit a policy,** go to **Policies** > **Firmware/Software** and click on the policy.
**NOTE** *Policy compliance is determined by comparing what is specified in a policy compared to what is being reported by Plantronics Hub.*

### Deploy a policy

There are four types of deployment: Optional, Persistent, Automatic and Silent (firmware only).

To deploy a policy, click SAVE. Changes will be initiated when the next polling cycle occurs
**NOTE** ***"Automatic" updates*** *If "Automatic" is selected for Deployment Type, the target device must be attached via USB at Plantronics Hub restart. See the appendix for products that support Automatic and Silent updates.*

### Deployment tips: Silent updates

Silent updates allow firmware updates to be applied after hours without requiring the user to initiate the update. Silent updates can have two different behaviors depending upon the type of device being updated.

**Behavior 1 | Devices that require "unplug/replug" after a silent update** In order to register an update (and, in some cases, to be recognized by Windows), some devices contain chipsets that must be "reset" following a firmware update which can only be accomplished by unplugging and replugging the device. Silent firmware updates for these devices are applied during the upgrade window as expected but the next user to log into that computer is prompted to unplug and replug the device. If the user does not do this, the update will not be registered. A list of the devices that have this requirement is listed in Appendix Silent updates: Devices that require "unplug/replug".

**Behavior 2 | Devices that do NOT require "unplug/replug" afer a silent update** The majority of Plantronics devices do not have the "reset" requirement. For these devices, updates occur during the specified window and upon completion, the update is registered. Users will not be required to do anything to the device at next login. This is applicable to all devices other than those listed in Appendix Silent updates: Devices that require "unplug/replug".

**Preparing for Success** Regardless of the device being updated, a successful update requires that the policy has been in place long enough (typically one polling cycle) to ensure all applicable Plantronics Hub systems have "checked in" and polled the server to find the update. Once the update has been found, it is stored on the system, waiting for all conditions to be met. The update attempts to run during the configured window daily until successful.

**Host System Requirements**

- Leave systems powered on and not in hibernation or sleep mode.

**Additional considerations**

- **Proxy** In a proxy environment, Plantronics Hub doesn't register a firmware update until the next user logs in.

### Delete a policy

To delete a policy, hover over the policy to reveal the Remove icon at the far right.

### Tips for firmware and software policies

- **Previous version limitations** If a user has a later version of Plantronics Hub than what is specified in a policy, the user is kept at the later version and not restored to an earlier version. Silent updates will not work for Hub clients prior to 3.10.2.
- **Apply latest version from Plantronics** With this version setting, updates are passed directly from Plantronics to the user.
- **Unlock a setting** Any setting changed from the default is locked, greyed out from the user's view in Plantronics Hub, with a note "Managed by IT administrator." To unlock the setting, edit the policy, change the value setting to "Retain User's Setting/Retain Device Setting." (This unlocks the setting but does not change it back to the original default value.)
- **Special mode settings** There are special mode settings for several products that can only be configured by the user, not by a policy. See the Appendix for details Special mode settings that can only be configured by the user.
- **Notifications for updates** You are notified via email or in **Home** > **Notifications** when firmware/software updates are available.
- **Test an update** Create a new policy for a specific group or user to test a firmware or software update. You can later edit the policy to extend to other groups or simply deactivate it.
- **Automatic file format detection** Three Windows formats (32-bit and 64-bit .msi and .exe files) are deployed with a software update; Plantronics Hub detects and downloads the correct format.

# Basics

## Change the polling cycle

The default Plantronics Hub polling cycle is six hours. During the first six months of installation, the recommended polling cycle is once every hour.

To change the polling cycle, go to **Policy** > **Software**. Click into a policy and open **Policy Overview**. Click the drop-down menu under TYPE and choose **Software Settings**. Within the **Policy Configuration** section, scroll to the bottom of the page and select **Administrator Settings** > **Polling Frequency**.

## Manage administrators

There are two administrative roles within this application: an admin with full privileges and an admin with read-only privileges. By default, the primary contact is the first admin to contact Plantronics. Administrators can be added locally or via Single Sign-On.

1. **To change the primary contact** go to **Admin** > **Accounts** > **Administrators** and clicking on the radio button under the Primary Contact column. There can only be one primary contact. This contact is initially setup to receive Plantronics Manager Pro email notifications.
2. **To change Plantronics Manager Pro email notification settings**, go to **Home** > **Notifications** > **Settings icon** (the icon to the right on the Notifications bar).
3. **To add/delete an administrator locally** go to **Admin** > **Accounts** > **Administrators**.
   You can also change admin roles and view account status.

## Single Sign-On (SSO)

Once configured, Plantronics Manager Pro can be accessed by selecting the Single Sign-on (SSO) button in the Plantronics Manager Pro login dialog (Service Provider-initiated) or can be accessed by selecting Plantronics Manager Pro from your list of IdP applications (IdP-initiated).

Both IdP-initiated SSO via SAML 2.0 and SP-initiated SSO are supported.

### Supported IdPs

We have tested and confirmed that Ping, Okta and ADFS IdP's can be successfully used with Plantronics Manager Pro. Other IdP's may work but have not been tested and therefore are not officially supported. Contact your Plantronics account representative or your Plantronics reseller to request support for a specific IdP.

**NOTE** *For additional support, view* our KB article on ADFS. .

### Configure SSO

In order to leverage enterprise SSO, first establish the necessary "circle of trust" between the Service Provider (e.g. Plantronics Manager Pro) and your organization's Identity Provider (IdP).

1. Go to **SSO** > **SSO Configuration** > **Service Provider (SP) Parameters** to download your Service Provider (SP) metadata file, then upload it to your IdP and set up the required attributes (alternatively, copy and paste the parameters).
2. Go to **SSO** > **SSO Configuration** > **Identity Provider (IdP) Parameters** Upload the metadata file from your IdP. Your SSO configuration updates accordingly.
3. Once IdP details are populated, go to **SSO** > **SSO Configuration** > **SSO status** and enable SSO.
   **IMPORTANT** *Notification that a user has been added to the IdP group associated to Plantronics Manager Pro is the responsibility of IT. SSO users will not receive an email from Plantronics Manager Pro. SSO users only appear in Plantronics Manager Pro after the first successful login.*

### Manage SSO accounts

Manage SSO user accounts in IdP but manage user roles and view account status in **Admin** > **Accounts** > **Administrators**.

- SSO accounts are READ-ONLY initally.
- Changing an SSO-only user to a PMP/SSO user will generate an email to that user requesting they establish an account. If the user had previously created a local account, an email will not be sent.

- If a user is deactivated from IdP, the user account remains visible in Plantronics Manager Pro until deleted.

## Change password

Click the drop-down menu next to your name at the top right of any page and go to **My Account** > **Account Password** to change your password.

## Configure your data retention policy

Plantronics Manager Pro stores all events and metrics for a given administrator, user, or device.

To configure your data retention policy, go to **ADMIN** > **Preferences** > **Data Retention Policy**. Elimination of data from the database can take up to ten minutes when deleting one or more years of data and then it is maintained on a daily basis.

**IMPORTANT** *Modifying the default retention period of "Retain Indefinitely" will automatically and permanently purge all data collected outside the specified period with the exception of the product name, serial number, and device first used date which will be retained in cold storage and will be retrieved in the event the device is reintroduced to the environment. This is done to ensure accuracy of the device first used date.*

# Reports, subscriptions and data

Plantronics Manager Pro provides a variety of reports and tools to help you analyze and manage Plantronics devices.

## Analysis Suite reports

| Report | Description | Subscription |
|---|---|---|
| **Asset Management and Adoption** | | **Provided** |
| Device Adoption | Examine adoption patterns of Plantronics products across your organization | |
| Device Distribution | View the distribution of devices among users, including Plantronics and non-Plantronics devices, and users without a detected device. | |
| Device Inventory | View total count and known status for all headset audio devices in your organization. | |
| Incompatible Products | Identify configurations of devices, softphones and Plantronics Hub versions with known compatibility conflicts. | |
| Policy Compliance | Monitor users' compliance with the firmware and software policies you have defined. | |
| Softphone Adoption | Examine adoption patterns of softphones across your organization. | |
| User Activity | Understand users' headset activity patterns, including headset calls made/received and call duration. | |
| Version Status | View the distribution of firmware and software across your enterprise as they relate to the latest versions available from Plantronics. | |
| **Call Quality and Analysis** | | **Subscription required** |
| Common Actions | Identify user behavior patterns related to mute, volume and Quick Disconnect functionality that may hold insights for training and performance. | |
| Conversational Analytics | Improve the quality of conversations by identifying individuals and/or physical locations where the % time of overtalk during conversations is higher than normal. | |
| Radio Link Quality | Analyze and troubleshoot radio link quality with Bluetooth headset to USB adapter connection metrics. | |
| **Health and Safety** | | **Subscription required** |
| Acoustic Events | Review history of acoustic events that occurred during conversations using Plantronics products. | |
| Noise Exposure | Identify Time-Weighted Average (TWA) configurations that may be causing user experience issues. | |

*** For a list of headsets that support the various reports, visit Supported Devices on Plantronics.com.**

## Subscribe

Plantronics Manager Pro and its suites are subscription-based. The Analysis Suite reports are provided with the installation of Plantronics Manager Pro as a one- or three-year foundational license; all other reports require subscription.

Contact your Plantronics reseller for information.

## Access reports

### Generate reports

Depending on the report, pie, bar, column and table charts are available to view and filter data.

1. To generate a report go to Library > All Reports and click on the name of the report you would like to generate.
   **NOTE** *If a sample report is generated, you are not subscribed to that dataset. Contact your Plantronics reseller for subscription details.*
2. Click directly on the graph for additional graphical and tabular views of the data.

### Apply filters

There are a variety of ways to filter and sort the data. Choose:

- Click directly on the graphical views
- Apply the filters on the left pane of each report
- Click on/off the graph legend (if available)

### Download results

In general, views can be downloaded in the format of .doc, .pdf and .csv.

To download graphical and tabular views of the data, click on the Download dropdown below the graph or table.

## API access

API access is granted with your foundational subscription to Plantronics Manager Pro. View Plantronics Developer Connection (PDC) site for details at developer.plantronics.com/.

## Link to partner applications

Partner applications can integrate with Plantronics Manager Pro via streaming or REST APIs to permit retrieval and sharing of data for supported Plantronics products within your organization. By enabling data sharing with selected applications, you are able to gain additional insights into your organization's usage and behaviors related to Plantronics products. Applications only appear if available in the region of the tenant.

**NOTE** *Additional configuration setup may be required based on the application partner. Contact the application partner or your reseller for more information on the application software license and Plantronics Manager Pro suite license required for solution interoperability.*

Depending on whether the application is an authorized Plantronics application or a custom application, choose:

- **Authorized Plantronics applications** Go to **Admin** > **Applications** > **Authorized Applications**, click the name of the application and click the toggle to enable data sharing.
- **Custom applications** Enabling data sharing is a two-step process for custom applications. To authorize the application go to **Admin** > **Applications** > **Pending Applications**and click "Authorize." Then go **Admin** > **Applications** > **Authorized Applications**, click the name of the application and click the toggle to enable data sharing.

# Troubleshooting

## Installation

| | |
|---|---|
| Some or all users are not showing up in the Plantronics Manager Pro tenant. | 1 Ensure that Plantronics Hub has been downloaded and deployed.<br>2 Ensure active internet connection.<br>3 Ensure that the user can get to an https website from their system. Use www.plantronics.com/ssltest for testing. Ensure port 443 is not blocked.<br>4 Ensure Plantronics Hub is connecting to the correct tenant. From the Plantronics Hub client, select Help > Support and expand the Troubleshooting Details section. All connection information can be found in this location. If the TenantID has a value of System, then Plantronics Hub is attempting to connect to our Consumer tenant, not your enterprise tenant. Once the Plantronics Hub software connects to a tenant, a user specific configuration file is created. If a connection to a tenant had happened previously then this file would exist and Plantronics Hub could get confused. Close Plantronics Hub, locate and delete the file called spokesuser.config found in C:\Users\<username>\AppData\Local\Plantronics or %appdata%. Restart Plantronics Hub. |
| How can I easily tell if Plantronics Hub has successfully connected to a tenant? | From the Plantronics Hub client select Help > Support and expand the troubleshooting details section. All connection information is housed in this area. |
| How does Plantronics Hub know which tenant to connect to? | Ensure you install the version of Plantronics Hub that is provided from within your tenant. Using the clients available from within your tenant will ensure the correct tenant connectivity. |
| What services/processes run at start up on the Windows operating system? | PLTHub.exe is the Plantronics Hub process that runs at start up providing all of the functionality expected from Plantronics Hub. PlantronicsUpdate.exe is also a process that runs at start up. This process allows Windows users without administrative permissions to upgrade Plantronics Hub. |
| Does Plantronics Manager/ Plantronics Manager Pro need to connect to my LDAP server? | Plantronics Manager/Plantronics Manager Pro does not directly connect to your LDAP or Active Directory servers. This information is passed to, and used by, the Plantronics Hub application for the purpose of user group identification. If the LDAP information is not populated, the Plantronics Hub application will attempt to auto-discover your LDAP server.<br>User groups in both Plantronics solutions are based upon LDAP queries. The creation of these user groups require a group name and a corresponding LDAP query. These LDAP queries are copied to the end users system in the form of JSON files. The Plantronics Hub application uses this LDAP information to run a query on the logged in user to determine that users LDAP attributes and to which group they might belong. |
| How often does the Hub client query LDAP? | LDAP is queried each time the Plantronics Hub software starts up. Also, during the normal poll cycle, if changes to any of the LDAP groups in Plantronics Manager has been detected, an LDAP query is initiated. |
| Where are the configuration files located? | **Windows**<br>~\AppData\Local\Plantronics**SpokesUser.config**<br>\ProgramData\Plantronics\Spokes3G**Spokes.config** |

| | |
|---|---|
| | **Mac**<br>~/Library/Application Support/Plantronics/Plantronics Hub/Plantronics/**SpokesUser.config**<br>/Applications/Plantronics Hub.app/Contents/Frameworks/Spokes3G.framework/Versions/A/Resources/**Spokes.config** |
| How is the Plantronics Hub installation language determined? | Plantronics Hub is installed in the language specified in the Windows "Regions and Languages" settings. When the locale is not supported, Plantronics Hub is installed in English. |
| How often does Plantronics Hub check for configuration changes? | This is called the polling interval and can be found in the Software Settings area of both solutions. This interval can be configured differently for each user group if needed. The default is every 6 hours. |
| What is the timeout for Plantronics Manager and Manager Pro? | The timeout is set to one hour. After one hour re-authentication is required. |
| Do I have to use Plantronics Manager Pro to host the update for my firmware and software? Can I use my own internal tools instead? | Yes and no. Updates to Plantronics Hub can be deployed completely independently of Plantronics Manager Pro. You can download the version of the .msi you need, and use your own internal deployment tools to push the update to your users. Firmware updates must be discoverable by Plantronics Hub and therefore Plantronics Manager Pro must be involved. But, during the configuration of a policy, you can change the default Deployment Source from "Plantronics Server" to be your own network share or web server. The path to this location must be entered into Plantronics Manager Pro. Plantronics Manager Pro will then inform Plantronics Hub that it must source this update from this new location. |
| Can Plantronics Hub be used in a proxy server environment? | Yes it can. If you are experiencing issues, please contact support. |
| Can I pass parameters to the .exe version of the Hub installer?<br>I don't know if my user requires 32- or 64-bit. | We do provide an executable version of the Plantronics Hub installation file that incorporates both the 32- and 64- bit .msi. Unfortunately, this file is not available preconfigured with your tenant parameters. To install using this .exe, you will need to pass these custom parameters as arguments to the PlantronicsHubInstaller.exe. Examples are shown below. You will need to identify the proper values for your tenant by reviewing Plantronics Manager/Pro > Admin > Accounts > Company Profile.<br>PlantronicsHubInstaller.exe TENANT_ID="Timbuktu" SERVER_URL="https://system-api.plantronicsmanager.com" TENANT_TOKEN="G1r6rM-xz7aV3oIM6fX89K5-RbnadmH2SkYZmd3S3aM26s1RxHT7YWeuzAjdNrPL" |

## Upgrading and updates

| | |
|---|---|
| Is there any way to allow Plantronics to directly notify my users of any available updates so that I don't have to be the gatekeeper? | Yes, select "Apply latest version from Plantronics" as the value for the Version field when defining your firmware policy. Selecting this option will allow Plantronics to notify your users directly when an update to their device becomes available. |
| How often does Plantronics release new software updates for Plantronics Manager Pro/ | We release two major updates a year and maintenance releases every 9 weeks as needed. |

| | | |
|---|---|---|
| | Plantronics Manager and Plantronics Hub? | |
| | Is it possible that all the users could receive an update notification and attempt to download at the same time? | It is highly unlikely. Plantronics Hub looks for updates based upon the Polling Frequency which is every 6 hours by default. The "countdown" is initiated based upon the start time of the Plantronics Hub process. |
| | I am no longer using Plantronics Manager/Plantronics Manager Pro. Now my users are not getting firmware/software update notifications. | Uninstall the enterprise Plantronics Hub version, install the consumer (.exe) version (plantronics.com/software) and users will continue to get notifications. |
| Functionality | | |
| | How does Plantronics Hub identify non-PLT devices? | Plantronics Hub will look at all HID devices that expose the Telephony Page (0xB). Devices that are determined to be a Telephony device with a VID (Vendor ID) not equal to Plantronics (0x47F) are inventoried and data sent to Plantronics Manager Pro. |
| | How does battery life get reported in Plantronics Hub? Some devices show talk time remaining while others show a percentage | There are hardware/firmware limitations across device families that don't currently allow Hub to report battery status in the same way for all products. Most of our bluetooth products have a calculated "coulomb counter" that reports remaining talk time in minutes. The DECT products currently report in very rough percentages only (e.g. 0, 25, 50, 75, 100). |
| | I've created a custom group and I noticed the users I added to this group are also in the "All Users" group. Which group will take precedence? | Custom groups will take precedence over the "All Users" group. |
| | Do firmware updates vary by region/country? | It could be that a firmware update contains a modification that only applies to a particular region/country but the update is made available to everyone. |
| | If I delete a User from Plantronics Manager Pro, is their Host and device deleted as well? | This answer varies based upon the device. Please review the following scenarios and the corresponding database implications:<br>**Plantronics devices**<br>Please note the following rules are true for all PLT devices:<br>• Devices with a serial number are never deleted physically (never deleted from database). Instead, these devices are "marked" as deleted<br>• Devices without a serial number are always deleted physically<br>IT deletes a user in Plantronics Manager Pro. What happens to the device and the host?<br>• If the device (with serial number) is registered to multiple users, it will not be deleted.<br>• If the device was only associated to the deleted user, then the host will be deleted as well.<br>• A device with no serial number will be deleted since there is no way to uniquely identify it and therefore no way of knowing if multiple users are sharing the device. |

- If the host is registered to multiple users, it will not be deleted.
- If the host was only associated to the deleted user, then the host will be deleted as well.

IT deletes a Host in Plantronics Manager Pro. What happens to the PLT Device and the user?

- Deleting the host, does not delete the device nor the user.

IT deletes a PLT device in Plantronics Manager Pro. What happens to the device and the Host?

- If the device is deleted from Inventory > Plantronics page, the device will be deleted (following rules above) regardless of how many users have the device registered.
- If the device is deleted from Inventory > Users page, the device will be deleted (following rules).
- The deletion of a device will not delete its associated host.

**Non-Plantronics Devices**

IT deletes a user with a non-Plantronics device from Plantronics Manager Pro. What happens to the non-Plantronics device and the host?

- The host will be deleted

IT deletes the Host, what happens to the Non-Plantronics device?

- The host will be deleted

IT deletes the Host, what happens to the Non-Plantronics Device and User A?

- Neither the host or the device will be deleted.

## Reports

| | |
|---|---|
| I paid for the Call Quality and Analysis/Health and Safety reports but the reports do not have any data. | To activate Call Quality and Analysis/Health and Safety reports, the device must be enabled to generate events and reports. To enable the device, go to **POLICY** > **Firmware (for that device)** > **Product Settings** > **Admin Reporting** and enable the specific report. |
| I don't see any of the headsets that are plugged into a DA70 or DA80. | Headsets plugged into a DA70 or DA80 will not show up in Inventory reports. |
| How frequently does Plantronics Hub send data to PMP? | Events are batched and sent at Plantronics Hub startup, then every two minutes thereafter. All other items, such as device registration, update status, etc., are sent immediately. |

## Infrastructure

| | |
|---|---|
| Who is the hosting provider? | Amazon Web Services |
| Where is the primary data being stored? | Data could potentially be stored in one of four AWS regions. Our AWS regions currently include US, Singapore, Australia and Ireland. The various regions provide us the ability to store Spokes data in locations that comply with local regulations. We are always looking to expand into new regions so please check our website for the most accurate information. |
| How is the multi-tenant application architected? | Due to privacy and security concerns, we cannot provide much information without a signed NDA. Using these MSDN definitions, our MySQL is "shared database, separate schemas", but our MongoDB is "shared DB, shared schema." |

| | |
|---|---|
| What language is Plantronics Manager, Plantronics Manager Pro, and Plantronics Hub written in? | Plantronics Manager and Plantronics Manager Pro are written in Java, Javascript and HTML. The Plantronics Hub client is written in C, C++, HTML and Javascript. |

## Security

| | |
|---|---|
| Is the data encrypted in transit between my company and AWS? Is the data encrypted when stored in AWS? | Data is encrypted in transit and at rest. |
| Can I get a list of the IP Addresses used so I can create firewall rules? | The Elastic Load Balancing (ELB) used by our cloud service provider scales as traffic load increases. It does this by increasing the number of interfaces (i.e. IP addresses) associated with the load balancer. Therefore we cannot provide a range or a set of IP addresses. It is recommended that you whitelist the URLs provided in our documentation. See "Configure your environment" in the Setup. |
| What data is collected by Plantronics Hub and sent to Plantronics Manager Pro? | This is covered in our privacy policy. |

# Appendix

## Update support

| | Not supported | Supported |
|---|---|---|
| **Automatic updates** | Blackwire 3xx<br>Blackwire 435<br>Blackwire 5xx<br>Blackwire 725<br>Blackwire 52xx<br>Calisto 6xx<br>MDA100<br>MDA2xx<br>MDA4xx | All other devices |
| **Silent updates** | | All devices (Windows only)<br>Blackwire 3xx*<br>Blackwire 435*<br>Blackwire 5xx*<br>Blackwire 725*<br>Blackwire 52xx*<br>Calisto 6xx*<br>MDA100*<br>MDA2xx*<br>MDA4xx* |

**** Requires unplug/replug after update***

*In order to register an update (and, in some cases, to be recognized by Windows), these devices contain chipsets that must be "reset" after a firmware update which can only be accomplished by unplugging and replugging the device. Silent firmware updates for these devices are applied during the upgrade window as expected but the next user to log into that computer is prompted to unplug and replug the device. If the user does not do this, the update will not be registered.*

## Events and supported devices

For an entire list of events and supported devices, visit Supported Devices on Plantronics.com.

## "Special mode" settings that can only be configured by the user

The products below support "special mode" settings. These settings can only be configured by a user and not by a policy.

**TIP** *The latest firmware version must be deployed for settings to be configurable by the user.*

**Blackwire 710/720**

- Mute reminder
- Language

**Voyager Legend**

- Answer/Ignore
- Caller ID
- Mute Off alert
- Mute reminder
- Language
- Wearing sensor
- HD voice
- Streaming audio

**Voyager Pro UC**

- Mute off alert
- Language
- Wearing sensor
- Streaming audio

# Support

## NEED MORE HELP?

**plantronics.com/support**


**Plantronics, Inc.**
345 Encinal Street
Santa Cruz, CA 95060
United States

**Plantronics B.V.**
Scorpius 171
2132 LR Hoofddorp
Netherlands





207469-06 (05.18)


plantronics