# Foresight User Guide

V1.1 2019 11 27

## Guide Table of Contents

# General Portal Admin

## Create a Foresight Space

The RealWear Foresight Support team will create a Foresight space for any customer who requests one, free of charge. Contact support@realwear.com with the following information:

- Name of your organization
- Name you desire as your space name (also known as domain name). The name can be up to 50 characters and may include spaces.
- First name, last name, and e-mail address of the person who will be the lead Foresight administrator for your organization.

Foresight Support will create the space and create a Tenant Admin account for your lead administrator. That person will receive an email from cloudadmin@realwear.com with login information and a temporary password. The lead admin will be directed to a password change page upon their first login.

## Foresight Portal Login

Tenant Admins and Tenant Admin Assistants may log into the Foresight portal. See the User Admin section of this documentation for more details.

The Foresight portal is at cloud.realwear.com.

If a user has forgotten their password, they may utilize the Forgot Password link on the login page to reset their password. The Tenant Admin may force a password reset on the User List page. See the User Admin section of this documentation for more details.

## Getting Support

The RealWear Foresight Support team will help with any questions or problems you have with the Foresight portal or cloud functions on the device.

The support team may be contacted at support@realwear.com

Alternatively, you may fill out a webform at https://www.realwear.com/contact-us. Select "Support Request" in the field labeled "Reason for contacting us?". Include the word "Foresight" in the message and the issue will be directed to our Foresight support team.

# Device Admin

## Device List Page

The Device List page is one of the most used pages in the Foresight Portal. It shows a table of all devices registered to your space with key information about the device including membership in device groups, compliancy to applied policies, last time checked in, and assignment to users.

The central feature of the Device List page is the list table with the following columns:

- Device Name: Name of the device as entered on the Device Detail Page. The text of the name serves as a hyperlink to this device's detail page.
- Device Group: List the device group or groups for which the device is a member
- Description: The Description of the device as entered on the Device Detail page.
- Last Checked In: The last time a device has sync'd to the Foresight system. If the device is registered, but has never sync'd, this cell will be blank.
- Last User Logged In: The last user who used the device.
- Firmware Build: A text string indicating the full build name of the device's OS version.
- Serial Number: This is the serial number as found on the device label and in the About Device app on the HMT.
- Compliance: The compliancy status of the device.
- Delete: De-registers the device from your Foresight space.

Devices may be filtered by any text string in the Device Name or in the Serial Number. To activate the search, select the search icon (magnifying glass). To remove a filter, delete any text in the search control and select the search icon.

Also, some categories such as Compliant or Sending may be selected from the select list.
If more devices fit the search criteria, the list will be split into pages. Use the First/Last, Page Forward/Page Backward, or Page Number links to move through the list.

## Device Detail Page

To view details about a particular device, select it from the Device List page.
The page is organized in sections:

- Device Info
- Device Configuration
- Device PIN
- Assign User
- Device Groups
- Policy Template
- Compliance Status
- Operations

### Device Info

After a device has been registered and sync'd for the first time, the Device Info section will populate with useful details about the devie:

- Description: As entered in the device creation.
- Platform: For all HMT devices, the value will be "Android+"
- Device Model: "RealWear inc. T1100G" for the HMT-1 and "RealWear inc. T1100S" for the HMT-1Z1
- Device Version: The Android version. Will be either 6.0.1 or 8.1.0 depending on the firmware loaded on the device.
- Serial Number: Android ID
- Device IMEI: For the HMT-1 devices, this is the serial number as found on the device label and in the About Device app on the HMT.
- Firmware Release: The long-text RealWear firmware build version as found in the About Device app on the HMT.

- Device Ownership: This will always be "Corporate"
- Device Rooted: This will always be "No" unless the device has been rooted in violation of the purchase terms of agreement. If rooted, the device's warranty is invalidated.

## Device Info (continued)

- On-boarding status with compliancy: This is not just the status of a device during the on-boarding, but also the compliance status to policies that the device belongs to. "Compliant" is the optimal status, indicating that the device has apps set up in agreement with all policies applied to the device.
- Last Checked In Time: The date and time when the device last checked in to the Foresight server. When active and connected to the Internet, the device will check in every 2 minutes.
- Current User: If a user is assigned to the device, the name will show here.
- MDM Agent version: This is the version of the RealWear Device Agent that connects the device to the Foresight cloud system.

## Device Configuration

This section holds data that was entered in during the device onboarding process or modified in this page afterward.

- Device Name: As added in the device registration process
- Identity (IMEI or Serial Number): The serial number of the device
- Email: As added in the device registration process or modified on this page
- MDM Type: Will always be "Enterprise Premium". Is not editable
- Description: As added in the device registration process or modified on this page

## Device PIN

With Foresight, the device may be locked with a PIN number remotely.

- User PIN: This option is deactivated until a user has been assigned. If a user is assigned, this option can lock the device with the assigned user's personal PIN. The admin will not know the user PIN number.
- PIN Override: Select this option to force a PIN number to the device, regardless of any user PIN that has been entered.
- No PIN: This is the default. The device will be accessible to any person whether via reboot or recovering from sleep mode and regardless of whether a user is assigned to the device.

Assign User

- Assign any person to the device. When selected, the user's name and email address will appear automatically.
- The user list is from the RealWear Identity System discussed in the Users section of this documentation.
- All users appear in the list. It is permissable for users to be assigned to multiple devices.
- When a user is assigned to the device, the User PIN radio button in the Device PIN section of the page will activate. If the selection is changed from assigned to "Unassigned" the User PIN radio button will deactivate and the No PIN option will be automatically selected.

## Device Groups

A device can be added to one or more Device Groups for easier management,

- Select the + Add Group button to bring up a list of available device groups. If the list is long, you may search for a text string contained in the group.
- Select one or more groups to which the device should be assigned.

## Policy Template

You may assign a policy directly to any device. While this functionality is available, RealWear recommends instead assigning devices to one or more device groups, thereby inheriting the Policy from the Group(s).

- Simply select the policy from the select list.
- Only one policy may be applied via direct policy selection.

### Compliance Status

Compliancy is the status between the state of the device and policies that have been applied to a device (whether directly or by association with a device group, user, or user group).

- The trigger select list only contains the default type of "no trigger".
- The policy type select list only contains the default of "Install Apps". Select Install Apps link to generate compliance report for apps on the device.
- When Install Apps is selected, all the apps on applied policies will show up in sub-sections. The sub-section header will have an icon designating the compliancy state.
- Select the app sub-section expand icon to see details about the app

Status Levels are:

- Compliant: The app and version on the device match the app and version in the policy
- Non-Compliant: The app and version do not match. This usually only occurs when an install has failed.
- In Progress: The policy has been sent to the device, but confirmation has not yet returned with Compliant or Non-Compliant status.
- Not Supported: This is not a valid state at this time in Foresight so this status won't occur
- Overriden: Overrides are not yet allowed in Foresight so this status won't occur.
- Inactive: A policy with this app and version has been applied to the device, but that app/version has been subsequently deactivated in the App Catalog controls.
- Unknown: Error in case communication between device and Foresight fails.

### Operation

This feature is currently under construction and testing. It may not appear for any device and information may be out of date.

## Add a Device - Manually

### Device Configuration

To add a new device, select *Devices* on the portal menu, then select the + *Add New Device* button in the upper left area of the page. The Device Detail Creation page will open.

- Device Name (required field): RealWear recommends using all or part of the serial number in the Device Name. For example, "West Yard #2 - MP6J309D7334455". Note that the last 6 digits of the SN are unique so a name such as "Mx Crew 15 - 456789" is also useful.
- Identity (IMEI or Serial Number) (required field): Currently serial number is the only accepted identity value. This is a 15 character alphanumeric string found on the device label, box label, or in the About Device app on the device. For example: "MP6J309D7334455"
- Email: Any email address may be used. This is for an organization's own reference and has no functional impact within Foresight.
- MDM Type: Leave the default "Enterprise Premium". This field is not activated at this time and has only one possible value.
- Description: Any text string will be accepted up to 200 characters. This Description will be used in the Device List page's search feature.

Refer to the Device Detail Page for information on how to set device PIN, users, device groups, and policies.

When all data is entered, select the Save button in the upper right area of the page.

A confirmation screen will appear reporting the results of the device add.

- Common issues are mistyping a serial number, leaving a required field empty, or attempting to register a device that has already been registered.

## Add a Device - Import

You may add multiple devices at once via the Import function.

- Download the import template by selecting the Import Devices button in the upper right area of the Device List page and then select the download link.
- The template is a .csv file and contains five fields:
    - Name - maps to Device Name on the Device Detail page
    - Identity - maps to Identity (IMEI or Serial Number)
    - Plan Type - maps to MDM Type
    - Asset ID - maps to Description
    - Email ID - maps to email
- Delete the sample data leaving the header row intact. Enter Name, Serial Number, and any other information desired to as many rows as desired.
- Remember that only the first two fields are required. The others may be left blank.
- You may name the file any title as long as it remains a .csv file.

- To register the devices, select Browse and then select the import file you created.
- The Upload button will appear when the file is selected. Press Upload to launch the import.
- The Foresight system will proceed line by line through the import file and report success when complete.
    - Note that if an error occurs on any line, the system will declare the failure and move to the next line.

## Device Groups List Page

RealWear recommends placing every device into at least one device group. This makes management of your device fleet much simpler.

To open the Device Group List page, select the Devices menu item and then the Device Groups tab at the top of the Devices page.

The central feature of the Device Group List page is the list table with the following columns:

- Group Name: Name of the group as entered on the Device Group Detail page.
- Description: Description for the group as entered on the Device Group Detail page.
- No. of Devices: A count of the devices that are members of the device group.
- Created Date: Date the device group was created
- Delete Icon: Erases the group from your Foresight space.

System Groups may show in your Device Group List. System Groups are created by RealWear Foresight administrators for use by organizations in their own spaces. Those system groups have policies that allow for easy application installation and ensures that updates will be automatically applied when they are loaded to the Foresight App Catalog.

For more information, see the System Groups and Policies section of this documentation.
To create a new device group, select the Add Device Group button in the upper right area of the Device Group List page. See "Using Device Groups" for information on the different elements of device groups.

# Using Device Group

Details in the Group Details section and the Policy Template section does not commit to the group until the Save button is selected on the page. Device additions or deletions to/from the group will save immediately, without need to select the Save button on the page.

## Group Details

Only two active fields exist for a device group and only one is required

- Name (required): Name the group with any text string up to 45 characters.
- Description: If desired, you may add descriptive information for the device group up to 200 characters.
- MDM Type: Leave the default "Enterprise Premium". This field is not activated at this time and has only one possible value.

## Devices

This section contains a table of all devices that are currently members of this group. If no devices are members, the table does not appear.

- To add a device or devices to a device group, the device group must be saved. If you select the Add Device button before saving the group for the first time, the system will execute a save then display the Group Members popup.
- Select one or more devices. When selected, each device will populate in the Added Devices column. Clicking an Added Device will move it out of the group.
- When the list of added devices is as desired, select the OK button. Otherwise, select the Cancel button to abandon any selections.
- The Group Members popup will close, and the device membership list will refresh to reflect the devices just added.
- To remove a device from the group, select the "x" symbol on the right end of the Devices table row.

## Policy Template

A device group have one policy template applied. Simply select the policy desired and save the Device Group page.

All devices that are members of this group will now have the selected policy applied.

# Apps Admin

One of the main functions of Foresight is to enable quick provisioning of applications to any device in your HMT fleet. The apps may be those your own company develops or purchases or they may be apps developed by RealWear development partners and approved for use by the RealWear Foresight team.

To administer apps, go to the App Catalog by selecting it from the main menu in the left margin. The app list will appear in the main screen. There are two categories of apps separated into two tabs:

- **Native Apps**: Loaded by a space's admin, these are apps that are either developed in-house by an organization or purchased directly.
- **Apps Posted by RealWear**: These are loaded and maintained by RealWear. This tab consists of two sub-groups of apps:
    - Apps developed by RealWear
    - Apps developed by RealWear's partner network

The Native Apps tab is the default view.

You may change the list type by selecting the Grid or List icons in the upper right area of the page.

## Add a New App

To add a new app, you must be in the Native Apps tab. Select the Add New App button in the upper right area of the page.

There are 3 main parts to the App Detail page:
- Application Details
- Version Details

### Application Details

The fields in the Application Details section will apply to all version of the app that will ever be posted.
- App Name (required): Any text string. This is usually the same name as the Android Label which is what you see on the screen under the launcher icon. However, there is no requirement that the App Name is the same as the Android Label of the app.
- Publisher Name: This is usually the name of the company or group that developed the app.
- Short Description: Max of 200 characters.
- Long Description: Max of 500 characters.
- Package Name: The Android package name. This field is non-editable. It will be populated automatically when the package is uploaded to Foresight.
- Active Status: This determines if the app will be able to be added to a policy and, thus, to a device. The default is "Active".

Graphics are not required but do make the application easier to interact with by admins.
- Hi-Res Icon: This is typically an image based upon the app's launcher icon but is higher-resolution and higher-fidelity. The optimal size is 512x512, although any square image will work. Rectangular images will have one dimension squeezed to fit into a square shape.
- Promotional Graphics: Up to five promotional graphics are permitted. It is usually best to use landscape images.

Note:
For the Hi-Res Icon, select the Upload Image link and attach the desired file.

For the Promotional Graphics, select the Add Images link and add all graphics at one time.

### Version Details

This is the section in which the APK is attached along with other version-specific information:

- Version Name: uneditable, will be added automatically from APK info.
- Version Code:  uneditable, will be added automatically from APK info.
- Posted By:  This will show on the App List page.  Can be any text.
- Published Date:  uneditable, will be added when the app version is saved to Foresight.
- Version Description:  500 characters max.
- App Status:  This should be named "Version Status".  If active, this version will be add-able to policies.  If inactive, the version will not be visible when adding apps to policies.
- Release Notes Text:  500 characters max.

To upload the app, select the button labeled, "Click here to select file" next to the Add App Package label.  Simply choose your APK and load it.  When loaded, the uneditable fields will auto-populate.

You still must select the Save button in the upper right area of the screen for the app to be committed to the App Catalog.

When the page is saved, the Version Details section will change to a table showing:

- Version Name
- Version Code
- Version Description
- Published Date
- Status
- Delete

## Adding New Versions of an App

After an app has been added, further versions may be added at any time.

- Select the app from the App Catalog
- In the lower right-hand corner, select the Add New Version button
- Add text to any of the editable fields.
- Select the "Click here to select file" button and attach the APK.
- Click Save to load the version to the App Catalog

Foresight will check to ensure that the version being loaded is unique.  It uses the Version Code property of the app.  If the version is not unique, an error will show and the APK won't be loaded.

After saving, the new version will be listed in the version table along with any other versions that have been previously loaded.

# Policy Admin

Policies are the method in Foresight by which apps are associated with devices. They connect devices, user, and apps allowing an administrator to manage devices around the world from any location.

## Policy List Page

The Policy List page is reached via the Policies menu item. It consists mostly of a single table listing all policies in the space. The table has the following columns:

- Name: As entered in the the new Policy Detail page
- Priority: A number indicating the priority of this policy in case a conflicting policy is attached to a device.
- No. of Policies: Number of apps loaded on the policy
- Users: Number of users to whom the policy has been applied
- User Groups: Number of user groups to whom the policy has been applied
- Devices: Number of devices to which the policy has been applied
- Device Groups: Number of device groups to which the policy has been applied
- MDM Templates: Type of license consumed by the policy. This field is not active in the current release so it has no functional impact
- Delete: Icon to delete the policy. If the policy is in use by users, user groups, devices, or device groups then the cell will read "In Use". The policy cannot be deleted when still in use.

## Policy Detail Page

### Policy Template Info

Three fields are included in the Policy Info:

- Name: Name of the policy as entered on the Policy Detail page.
- Description: Description of the policy as entered on the Policy Detail page.
- Priority: Any integer from 1 to 200. Resolves conflicts when more than one policy applies to a device.

Priority is a unique number from 1 to 200. The uniqueness is enforced via a select list that shows all other priorities occupied and the name of the occupying policy. Conflicts occur solely when an uninstall action and an install action for the same package exists on the same device. In that case the policy with the highest priority will prevail (lower number is higher priority - priority 1 is the highest possible).

### Apps

The Apps section contains the Policy App List in which all apps and versions in the policy are listed. The following fields are included:

- Title: The App Name as entered on the App Detail page.
- Version Name: as entered on the App Detail page
- Short Description: this is the Short Description of the application, not the the version
- Posted By: as entered on the App Detail page
- Package Name: as entered on the App Detail page. This is the unique identifier for this app. An example is com.realwear.barcode
- Action: Either Install or Uninstall. Selected during the addition of the app to this policy
- Latest Version: Indicates whether the currently attached version is the latest version available for this app.
- Delete: Icon to allow deletion of the app from this policy.

# Creating a New Policy

To create a new policy, launch a new Policy Detail page by selecting the Add New Template button in the upper right area of the Policy List page.

## Policy Template Info

- Fill in the Name field. This is a required field. Any text up to 100 characters is allowed.
- Fill in the Description field if desired. Any text up to 200 characters is allowed.
- Select the Priority (required): This is an integer between 1 and 200 and is set via a select list. The default is the one number higher than the highest occupied value for this space. In other words, the default is for any new policy to be the lowest priority by one place. If you have several policies on your space and the policy with the highest number/lowest priority has priority of 105, the new policy will default to priority of 106.

## Apps

A policy does not technically require an app, but it won't have functionality until at least one app is attached.

- Select the Add App button in the upper right area of the Apps section. If the new policy has not yet been saved, the system will perform an auto-save.
- Select the App and Version from the Select an Application. Note that all apps and all versions available to your space will appear. Apps Posted by RealWear will show, in alphabetical order, first followed by your own Native Apps.
- After selecting the app, the page will refresh and auto-populate the non-editable fields
- User Confirmation Needed defaults to "No". This is the recommended setting so that end users don't need to accept app installation or upgrade commands on the device.
- Application Action defaults to "Install". Selecting "Uninstall" will cause the application to be uninstalled on the device.
- Click "Add" to save the app or "Cancel" to abandon this page.

After adding the app to the policy, the Policy App List table will refresh with the results of the newly added app included.

If the policy has been saved (or auto-saved) it is not required to save the Policy Detail page after adding an app.

## Modifying an Existing Policy

Existing policies may be edited at any time. When modified, any material changes such as added apps, removed apps, or change policy priority will take effect immediately.

To place a higher priority on the policy, an unoccupied priority must exist. Sometimes it is necessary to go to other policies and move their priorities to make space for another policy priority.

To delete an app from the policy, use the delete icon, an X at the right end of the row in the Policy App List table. Note that the removal of the app from the policy does not remove the app from any device governed by the policy. In order to remove the app from a governed device, open the app from the Policy App List table and change the action from "Install" to "Uninstall".

If Policy Template Info has been changed, the policy must be saved before exiting. If only apps have been changed, no saving is required.

# User Admin

There are three user roles in the Foresight portal:

- Tenant Admin: Every Foresight space (or tenancy) must have one and only one Tenant Admin. This person is the primary contact to RealWear for Foresight-related communications. Many organizations have a service account in this role such as foresight.admin@company.com. The Tenant Admin can perform every function on the Foresight portal.
- Tenant Admin Assistant: Each space may have as many Tenant Admin Assistants as desired. The Tenant Admin Assistant can perform every function that a Tenant Admin can with the exception of creating/modifying/deleting Tenant Admin or Tenant Admin Assistant accounts.
- User: Users do not have logins to the portal. They are, in fact, device users only. They may be assigned to devices and may create PIN numbers for their account.

## User List Page

The User List Page is the first page in the Users menu. You may need to expand the Device Management group in the left margin menu to access the Users menu item.

The User List page mostly consists of the User List table. This table contains all the users managed in Foresight.

Columns in the table are:

- Check box: Chose these to perform bulk actions on users
- Username: This is a concatenation of the First Name + Last Name of the user.
- Email / Username: This is the email address only.
- User Groups: A commas separated list of all groups to which the user is assigned.
- Last Login Date: The most recent date and time a user was logged into and using a device that sync'd to Foresight. This is not the last login datetime of a Tenant Admin or Tenant Admin Assistant on the portal.
- Status: Onboarding status only for users who have been assigned devices. It does not reflect activity on the Foresight portal by the Tenant Admin or Tenant Admin Assistant.
- PIN Refresh: An icon of circular arrows indicates that a personal PIN has been set up by a user. If the user forgets that PIN or simply wants to change the PIN, a Tenant Admin or Tenant Admin Assistant may press this link to have a PIN change email sent to that user.
- Delete User: An icon of an "X" will delete the user (after confirmation) from the Foresight identity store.

The search controls at the top of the screen allow for searching of any test string in the user's name or email address. Users can also be filtered by their compliancy status.

## Tenant Admin Account

The RealWear Foresight Admin team creates and manages all Tenant Admin accounts. The first name, last name, and email address are all that is required for the Tenant Admin account. This information will be requested anytime a space is created in Foresight.

When any new user is added, that user will receive a welcoming email. Since the Tenant Admin is an admin account with access to the portal, there will be a login url and a default password password provided. The Tenant Admin, when logging in for the first time the system will require a password change.

Contact support@realwear.com to modify the name and/or the email address of the contact. When the account information is modified, the Tenant Admin will receive notice from the Foresight system, cloudadmin@realwear.com, confirming the change. If the email address is also changed, an email will be sent to both the current email and new email addresses as confirmation.

Although the Tenant Admin is a special role, that account may also be a device user. Therefore, the User Groups and Policy Template sections are actionable. These sections are not required for the Tenant Admin. Also note that the Role select list is non-editable with the value "Tenant Admin" locked in by default.

## Tenant Admin Assistants Accounts

The Tenant Admin is the only user that may create or modify a Tenant Admin Assistant accounts.
To create a new Tenant Admin Assistant:

- Log in as Tenant Admin
- Navigate to the User page by ensuring the Device Management sub-menu is open in the left margin menu bar, then select Users to open the User List Page
- Select the Add New User button to open the Add New User page.
- Enter First Name, Last Name, and Email Id (Email Address). These are all required.
- MDM Type is a non-functional field at this time. It defaults to Enterprise Premium.
- In the Role select list, choose Tenant Admin Assistant.
- Select Save when entry is complete

After saving, the portal will return to the User List Page and the table will refresh to reflect the user added. Existing accounts with User roles may be modified to Tenant Admin Assistants. Only the Tenant Admin may perform this action. All existing group and policy assignments will remain in effect for that account.

When any new user is added, that user will receive a welcoming email. Since the Tenant Admin Assistant is an admin account with access to the portal, there will be a login url and a default password password provided. The Tenant Admin Assistant, when logging in for the first time the system will require a password change.

Although the Tenant Admin Assistant is a special role, that account may also be a device user. Therefore, the User Groups and Policy Template sections are actionable. These sections are not required for Tenant Admin Assistants.

## User Accounts

In Foresight, users are device users. They can be created and managed by either at Tenant Admin or Tenant Admin Assistants.

To create a new standard User:

- Log into the Foresight portal as either Tenant Admin or Tenant Admin Assistant
- Navigate to the User page by ensuring the Device Management sub-menu is open in the left margin menu bar, then select Users to open the User List Page
- Select the Add New User button in the upper right-hand corner to open the Add New User page.
- Enter First Name, Last Name, and Email Id (Email Address). These are all required.
- MDM Type is a non-functional field at this time. It defaults to Enterprise Premium.
- In the Role select list, leave the value as the default "User".
- Select Save when entry is complete

During the initial creation of the user, the account may be assigned to one or more user groups and/or a user policy.

- Select the Add Group button to choose user groups to which the account will belong
- Use the Change Template select list to add the user to any policy.

*Note:*
RealWear recommends that user policy assignments be done via user groups and not directly on the user account. This will allow for easier management of users as the population grows and evolves.

## User Groups

Like device groups, user groups make managing the Foresight space easier over time. RealWear recommends that assignment of policies to users always goes through User Groups.

To create a new user groups:

- Log into the Foresight portal as either Tenant Admin or Tenant Admin Assistant
- Navigate to the User page by ensuring the Device Management sub-menu is open in the left margin menu bar, then select User Groups tab to open the User Group List Page
- Select the Add User Group button at the upper right-hand corner to open the User Group Detail page.
- Enter the Group Name. This is the only required field.
- Enter a Description if desired.
- MDM Type is a non-functional field at this time. It defaults to Enterprise Premium.
- Users may be added by selecting the Add User button and selecting from the existing list of users. If the Add User button is selected before the group has been initially saved, the system will auto-save the group before opening the group members popup.
- If desired, select a policy for this user group from the Change Template select list in the Policy Template section.
- If the group has not been saved or auto-saved, make sure you select the Save button before exiting.

# Activity Log

The Activity Log page is a useful tool to understand what activities have occurred in Foresight. The log shows activity for the following system objects:

- Users
- User Groups
- Devices
- Device Groups
- Policies

Any creation, modification, or deletion of any of the above items will show up on the Activity Log.

By default, only logs from today will show on the initial page load. You may filter the log in the following ways:

- Search for a text string within Name or Description fields of a device, policy, or user field including the first name and last name of a user. After inputting a text string, you must select the search icon (looks like a magnifying glass) to execute the search.
- Select a specific type of activity log - user, device, or policy - for the select list. The search will run automatically when a selection is made from the select list.
- Select a specific date from the calendar-day picker. After setting the date filter, the search will rerun automatically.
- Select all dates by selecting "clear" next to the calendar control. After clearing date filter, the search will rerun automatically.

## Dashboard

The dashboard shows some basic information about your device fleet, but is not yet optimized. Some information may not be updated regularly.

# Device User Experience

The Foresight experience of managing HMT devices is designed to be mostly headless from the user who's wearing the devices' perspective (meaning there is almost no user interface for the wearer to operate). Instead, the background RealWear Device Agent takes instructions from the Foresight server via the Internet and then performs configuration changes on the device.

## Foresight System Messages

Some messages and notifications will be visible to the wearer as the background actions occur. These include:

- Activity icons in the status bar. These are in the shape of a RealWear "W". More than one may occur at a time. This icon indicates that data is being downloaded by the device. The icon will disappear automatically when the data transfer has completed.
- Toast notification of about 2 seconds in duration when performing download, ongoing app installation, and successful app installation. These toast messages are in gray ovals at the bottom of the screen and disappear automatically. Different application or device agent app names will be included in the toast messages
- Notifications in My Notifications will appear as apps are installed successfully. They will remain active until the device is rebooted. The user may dismiss the notifications, but that is not required.
- Device de-registration cleanup message will show when a device that has been registered to a Foresight space is deregistered. This is a toast and will disappear automatically after about 2 seconds.

## App Installs

Devices check into the Foresight server approximately every two minutes when connected to the Internet. It is a low-volume data transfer so users won't notice the check-in. There is no UI confirmation that this check-in has occurred.

When a policy change results in an app install, upgrade, or removal - it may take a few minutes for the change from the portal to move through the message queue and then download app files.
If the device is in the My Programs page when an app is initially installed via Foresight, the page will not automatically refresh (although the toast message will appear briefly indicating successful installation). To see and launch the app, you must exit the My Programs page and then return.

## Upgrades When App is In Use

There is one instance in which user intervention is required. When an existing app is open and an upgrade is sent to the device, the device agent will inform the user that the upgrade is available. The user is given the option to exit the application immediately and accept the upgrade or to defer the upgrade for a set amount of time. If the later is chosen, the user may continue working in the app.

Note that the user cannot permanently avoid the upgrade. It must be performed at some point, ensuring that the device attains compliancy in a reasonable time period.