



# Fleet Access Manager

USER GUIDE

## Table of Contents

Table of Contents	2
Copyrights	3
Definition of “Device”	4
Virtual Care System	5
Teladoc Health Fleet Access Manager Overview	6
Users	12
Devices	24
Locations	45
Organizations	53
Programs	54
Practices	62
Services	67
HIPAA	72

## Copyrights

© Teladoc Health, Inc. All rights reserved.

This manual contains information including, but not limited to, instructions, descriptions, definitions, firmware and software, which are proprietary to Teladoc Health.

Copyright information is protected under Title 17 of the United States Code. This information shall not be copied, modified, or used in any manner that violates any rights of Teladoc Health.

We will strictly enforce all of our rights.

### Patent(s):

<https://teladochealth.com/patents/>

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

Last updated: February 2024

## Definition of “Device”

Use of the word “device(s)” in this User Guide refers to Teladoc Health telehealth products, not medical devices as defined in Section 201(h) of the Federal Food, Drug, and Cosmetic (FD&C) Act.

In addition, the term “mobile devices” refers to smartphones and tablets.



## Virtual Care System

Health systems view virtual care as an extension of their services, relying on a combination of software, hardware, networks, systems and people to work together to deliver improved access and care to their patients.

Enabling healthcare's only integrated virtual care platform, Teladoc Health powers virtual encounters at clinics, healthcare facilities and patient homes for an integrated experience across a multitude of use cases. Built on our cloud-based network, Solo™ is the backbone to delivering care anywhere at any time. It provides users with everything they need to streamline their telehealth needs for fast user adoption.

### **Designed for healthcare, security and reliability**

Our cloud-based, patented network ensures the industry's highest standards for protecting and securing sensitive healthcare information. Our downloadable and web-based platform allows users to access virtual care across a broad range of consumer and telehealth devices in a variety of clinical environments.

## Teladoc Health Fleet Access Manager Overview

Fleet Access Manager may be used for configuring and managing users, Teladoc Health devices, locations (hospitals), and organizations in your telehealth program. You can choose who has Fleet Access Manager access for your account.

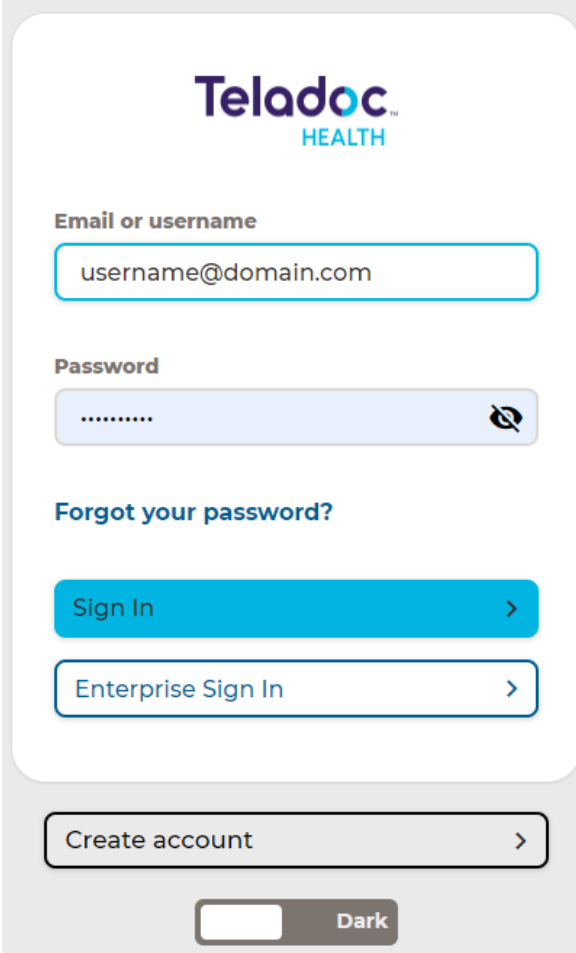
Note: Any and all names used in this document are only used as examples. They do not represent true persons.

### Tenant Definition

A Tenant is a logical representation of a customer instance within the Solo platform.

## Logging In

1. Open your browser and enter <https://fleetaccessmanager.intouchhealth.com>. When you do, the following will be displayed:



The screenshot shows the Teladoc Health login interface. At the top is the Teladoc Health logo. Below it are two input fields: 'Email or username' containing 'username@domain.com' and 'Password' with a masked password '.....' and a toggle icon. A link 'Forgot your password?' is positioned below the password field. There are three buttons: a blue 'Sign In' button, a white 'Enterprise Sign In' button, and a white 'Create account' button, all with right-pointing chevrons. At the bottom is a 'Dark' mode toggle switch.

2. Enter your username and password.
3. Click **Sign in**.

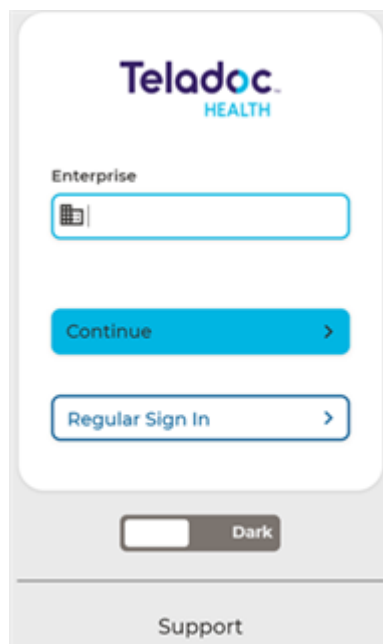
## Enterprise Login

Enterprise login is for hospitals provisioned by Teladoc Health to use hospital credentials.

Note: If you log into Fleet Access Manager using Federated Authentication, then "idprovider.intouchhealth.com" will need to be whitelisted in your external authentication provider instead of just "idprovider.intouchreports.com".

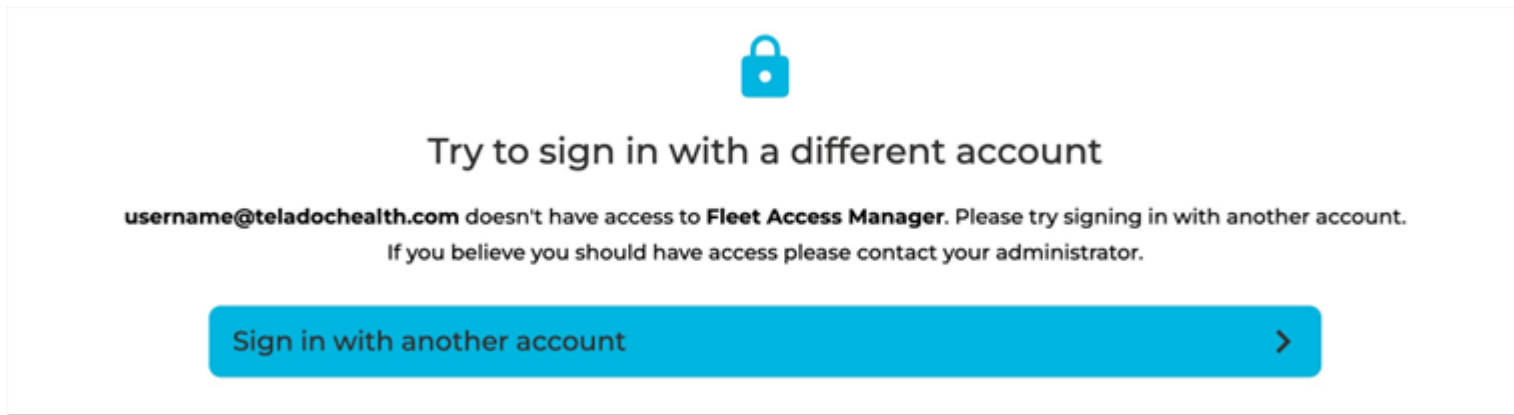
Note: Customers who distribute SSM enterprise systems can install a Mac version of the Teladoc Health Desktop App that will not auto-update.

1. On the login page, click Enterprise Sign in near the bottom of the page.
2. Enter the domain name provided to you by Teladoc Health.
3. Select Continue.
4. Sign in using your hospital credentials.



## Login Issues

If you have more than one Teladoc Health account and you use an account that is not authorized to access the Fleet Access Manager, the following will be displayed.

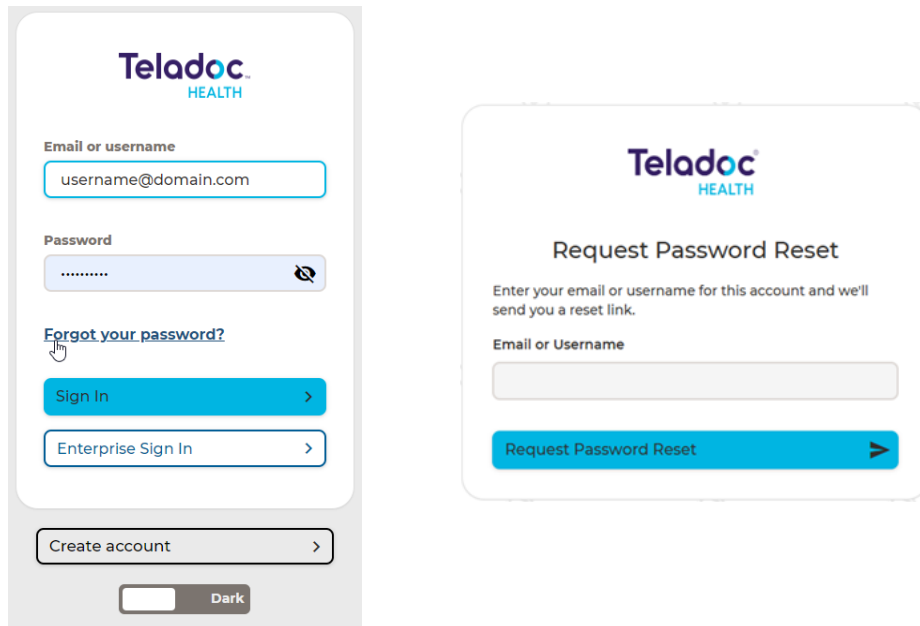


Click [Sign in with another account](#) and log in with the correct account.

## Forgot Password

If you know your Username or email, but forgot your password click [Forgot your password?](#)

If you don't know your Username or email, call Technical Support or open a chat session by clicking the [Chat with a Live Agent](#) link. Once you have your Username or email, click on [Forgot your password?](#) to open the Reset Password page.



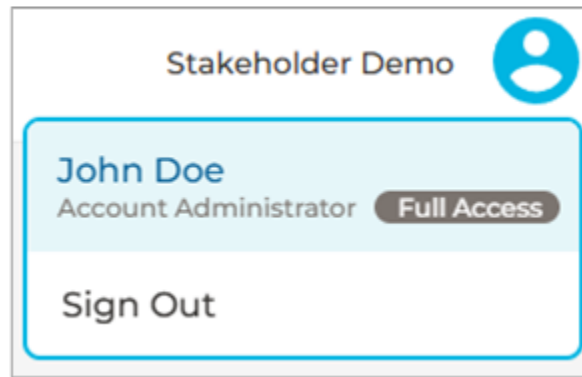
The image shows two screenshots of the Teladoc Health user interface. The left screenshot is the main login page, featuring the Teladoc Health logo at the top. Below the logo are two input fields: 'Email or username' containing 'username@domain.com' and 'Password' with a masked password and a visibility toggle. A link for 'Forgot your password?' is highlighted with a mouse cursor. Below these are three buttons: 'Sign In', 'Enterprise Sign In', and 'Create account'. At the bottom, there is a 'Dark' theme toggle. The right screenshot is the 'Request Password Reset' page, also with the Teladoc Health logo. It contains the text 'Request Password Reset' and 'Enter your email or username for this account and we'll send you a reset link.' Below this is an 'Email or Username' input field and a 'Request Password Reset' button.

Enter your Username or email address and click Continue. A link will be sent to your email. Open the email you receive, click the link provided, and follow the instructions.

## Logging Out

To log-out follow the instructions below.

1. Select the user icon in the upper right-hand corner of the Window.
2. Select Sign Out.



## Export CSV Reports

You can create a CSV report of the current table with any filter or sort applied by clicking Export CSV in the upper right-hand corner.

**Users**  
Manage the users in your telehealth tenant.

Active users: 246 | External users: 0 | Deactivated users: 7

Search [ ] [X] Search [ ] Deactivate users [ ] Create User + [ ]

**Export CSV** [ ]

<input type="checkbox"/>	Name	Type	Specialty	Email	Username	NPI	
<input type="checkbox"/>	Aaron Blake	Admin	Administrative	new_aaron_blake_6286@maili...	aaron4815		<span>Active</span> ...

## Users

On the Users page you can view, add, activate, deactivate, and edit users; this includes configuring device access for users in your organization. Sort the table by any column, with the exception of except Type and NPI (National Provider Identifier).

Column	Description
Name	The user's full name. Click their name to display their care locations.
Type	The type of user, which can be User, Admin or External.
Specialty	The user's specialty. It can be selected from a list of general and Tenant-specific items
Email	The user's email address.
Username	The user's username
NPI	The user's National Provider Identifier.
Status	The user's status which can be Active or Deactivated
...	Click the ellipses to start a reset password flow for the user

## User Types and Definitions

### Customer Admin



A customer admin, also known as a full access admin, is a role designated by a customer for one of their employees within a Tenant that has a broader permission set than a typical user. A customer admin is typically the customers' telehealth administrator.

#### **Customer Read-Only Admin**

A customer read-only admin is a second role designated by a customer for one of their employees. This role would be within a Tenant and has a broader permission set than a typical user. A customer read-only admin is able to view a telehealth program in Fleet Access Manager, but is unable to make changes to the account. For example, a customer read-only admin can't edit users or grant access to users or devices, and doesn't have permissions for any non read-only features.

## External

A user which is not part of the Tenant, and who still has access via access rules or programs to one of the devices which is part of the Tenant.

## Device Access

A policy that allows a user to connect to a telehealth device. Access can be grant one to one using Access Rules or it could be granted in groups as part of an All-Access program.

## Adding Users

### Regular Users

1. Click Users in the left navigation panel.
2. Click “Create User +” in the upper right-hand corner.
3. Enter the user's first name, last name, and email address.
4. If you do not use Federated Authentication, enter the user's username.
5. Select the Organization from the dropdown.

The screenshot shows a 'Create User' form with the following fields and options:

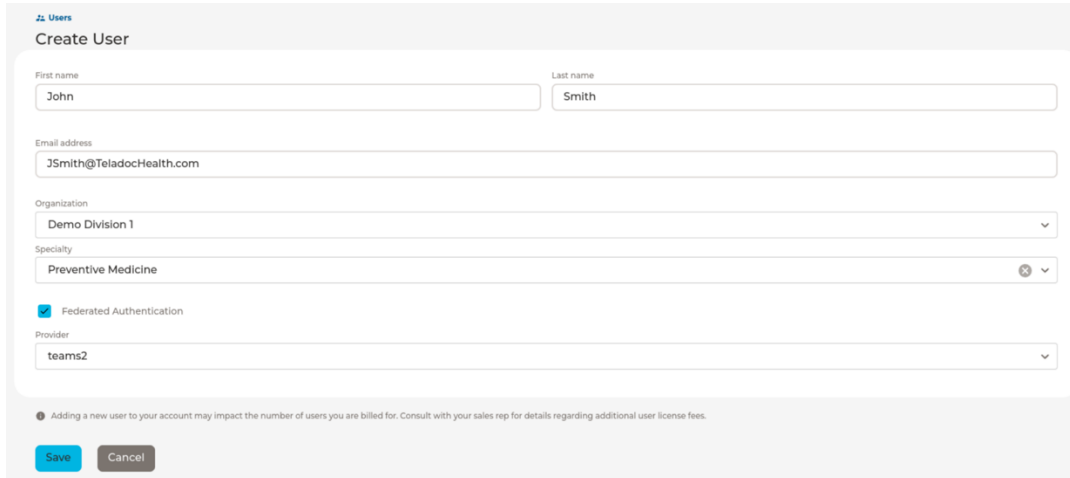
- First name** and **Last name**: Text input fields.
- Email address**: Text input field.
- Username**: Text input field.
- Organization**: Dropdown menu with 'Demo Division 1' selected.
- Specialty**: Dropdown menu with 'Choose' selected.
- Federated Authentication**: A checkbox option.

At the bottom of the form, there is a note: "Adding a new user to your account may impact the number of users you are billed for. Consult with your sales rep for details regarding additional user license fees." Below the note are two buttons: 'Save' and 'Cancel'.

## Federated Authentication Users

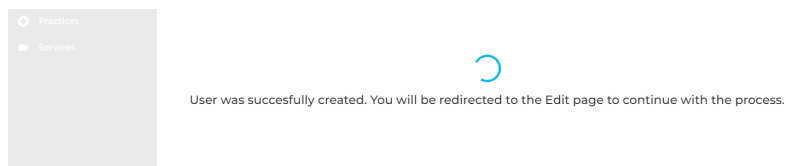
If the user logs in through Enterprise Authentication, select Federated Authentication and then select the Federated Authentication provider from the dropdown.

**Note:** When you create a new enterprise user, Fleet Access Manager will create a temporary username. When the enterprise user first logs in their temporary username will be replaced by their final username.

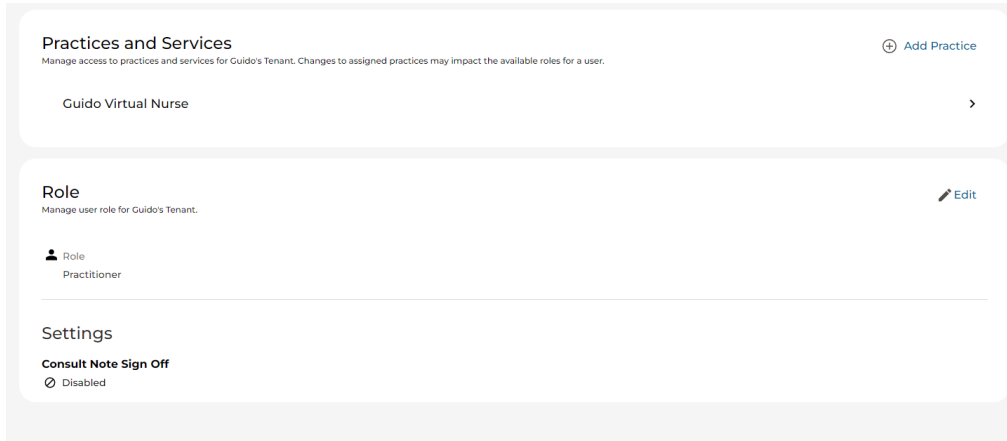


## Adding a new user to Practices and Services

After successfully creating a new user, next add them to one or more of your Practices and, optionally, Services.



1. Click "+ Add Practice". From the dropdown menu, select one practice for the new user.
2. Optionally, you can include the user in specific Services by choosing from the Services dropdown
3. You can continue adding Practices and Services, if available, to the user by clicking "+ Add Practice" again and following the steps above.
4. Add the user's Role from the available ones for all the practices the users was added to
5. Optionally, you could update Consult Note Sign Off setting for the user, this option is only available for certain roles, if the role assigned to the user is not meant to be able to sign consult notes the option will be disabled.



Note: When you create a new user and add them to one or more Practices, you have the option skip adding them to any Services initially. You can always come back later to add the user to specific service through the service member options within the Practice.

### Password Reset

After adding a non-federated user a password reset needs to be triggered so that the end user can choose a new password a start using Solo

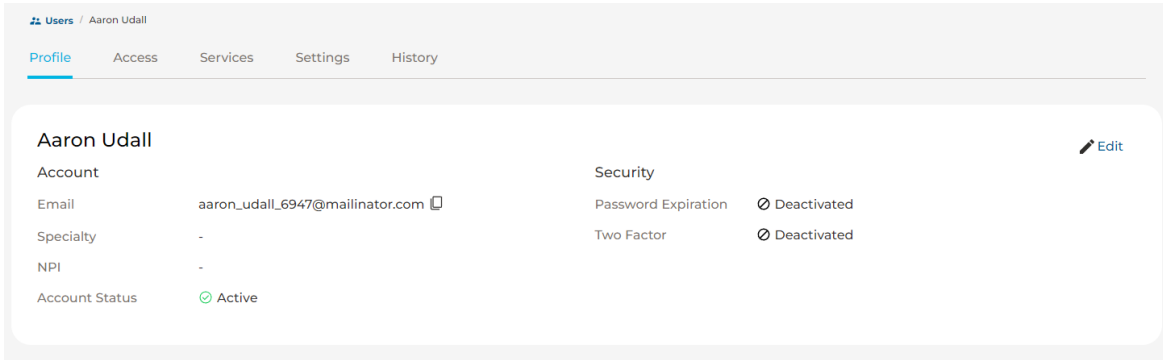
1. Locate the newly created user in the users index page
2. Click the ellipsis
3. Click Reset Password

Aaron Matthews Rivers	Admin		aaron_rivers_9602@mailinator.c...	aaron6640	Active	...
Aaron Nelson	User	Cardiology	aaron_nelson_841@mailinator.co...	aaron6690	Active	...
Aaron Rivers	User		aaron_rivers_5488@mailinator.c...	aaron9015	Active	...

## Edit Users

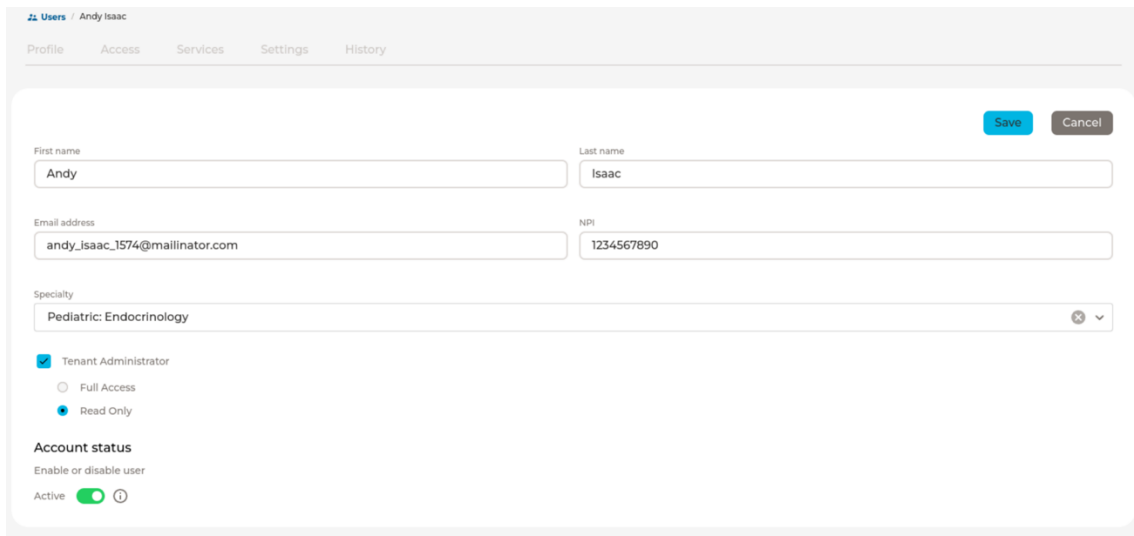
Note: Only Full Access Administrators can edit users.

To edit a user click the row of the user you want to edit. User edition is divided into tabs including Profile, Access, Services, Settings, and History



### Profile

The user profile tab contains basic information about a user.



- First Name: The user’s first name
- Last Name: The user’s last name
- Email: The user’s email address
- NPI: The user’s National Provider Identifier number

Tenant Administrator: By enabling this option the user becomes an administrator that can use Fleet Access Manager to manager this Tenant with the access level given. The available access levels are Full Access and Read Only

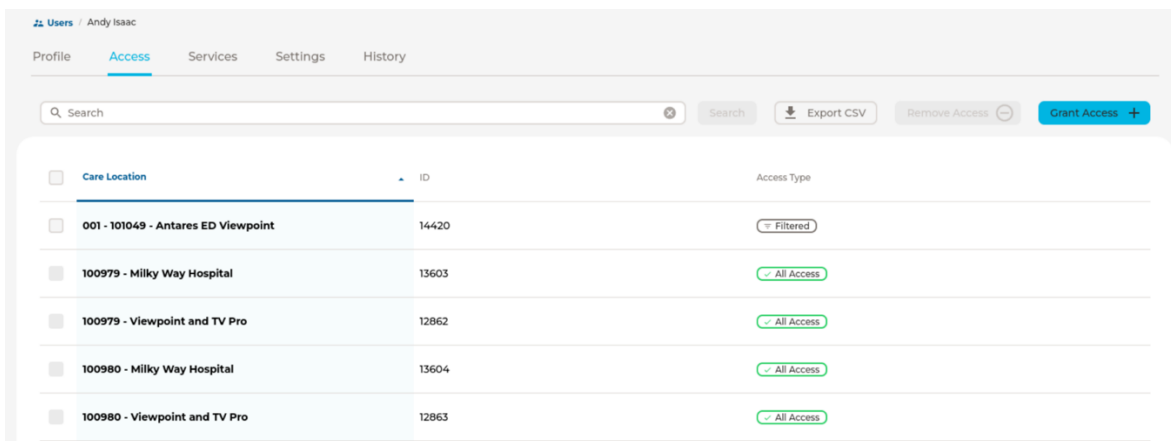
Account Status: Users can be active or deactivated. Deactivated users cannot log into Solo

Under “Security” there are two read only fields that are not shown in edit mode.

1. Password Expiration: If the user has password expiration enabled
2. Two Factor: If the user has two factor authentication enabled

### Access

The user access tab shows all the devices the user has access to and the type of that access. The available access types are Filtered, for access granted specifically to a single device, and All Access, for group access granted via an All Access program.

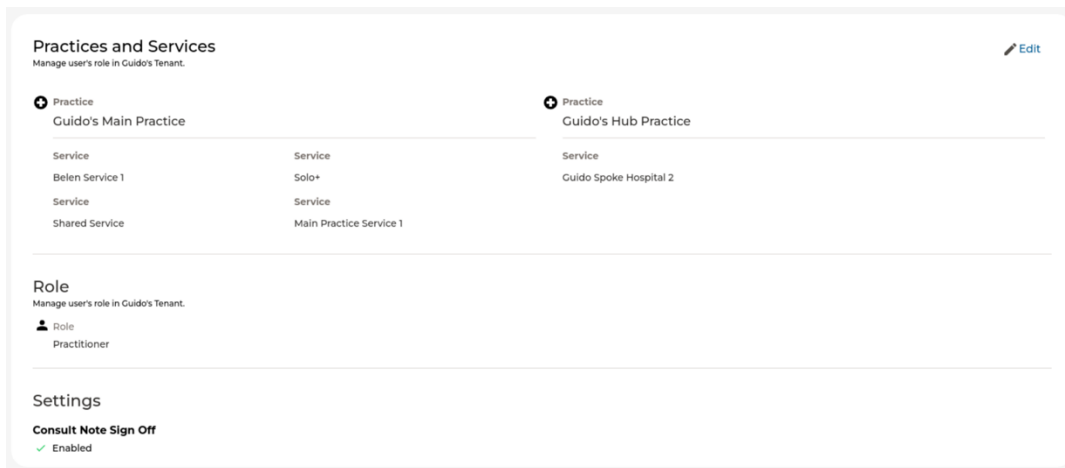
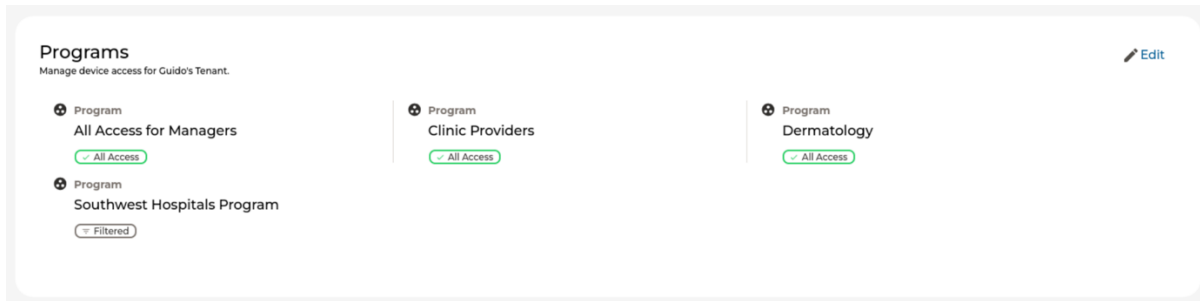


Filtered access can be granted by clicking on the “Grant Access +” button and removed by selecting the access and clicking the Remove Access button. More on this topic can be found in the access section

All Access type access is read only in the access tab of the user edit page.

### Services - Programs

The service tab shows the Programs that the user is a part of and the Practices and Services that the user is associated with. Programs, practices, and services can be added or removed from the user



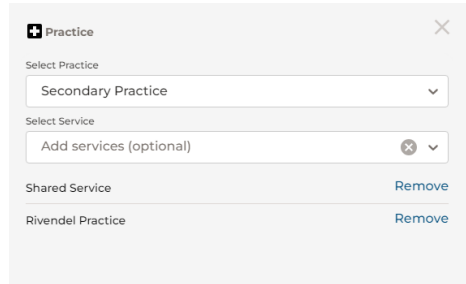
To add or remove programs the user is a part of:

1. Click edit
2. To add new programs to the user click the programs dropdown menu and choose any number of programs the user will be added to
3. To remove existing programs click the x next to the name

### Services - Practices and Services

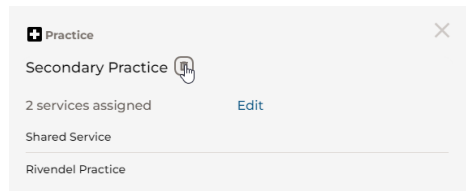
To add or remove practices or services a user is part of:

1. To add a practice, click "+ Add Practice"
2. In the side panel choose the desired practice, optionally add any desired service the selected services are listed below the practice and service dropdown



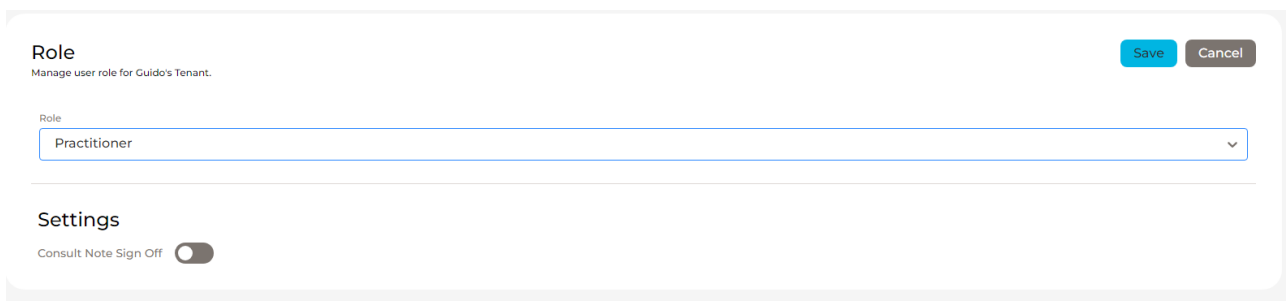
To add or remove services find the practice that the service should be accessed from and click it displaying the side panel

1. Click “Edit” and select the service from the service dropdown
2. To remove a practice, click practice row to display the side panel then click on the trashcan icon and confirm when prompted



To select or update a user’s role in its practices:

1. Click edit in the role section
2. Choose one of the available roles
3. (Optional) Update the Consult Note Sign Off setting. Consult Note Sign Off may get disabled if the user’s role is updated to one that does not allow Consult Note Sign Off to be enabled.

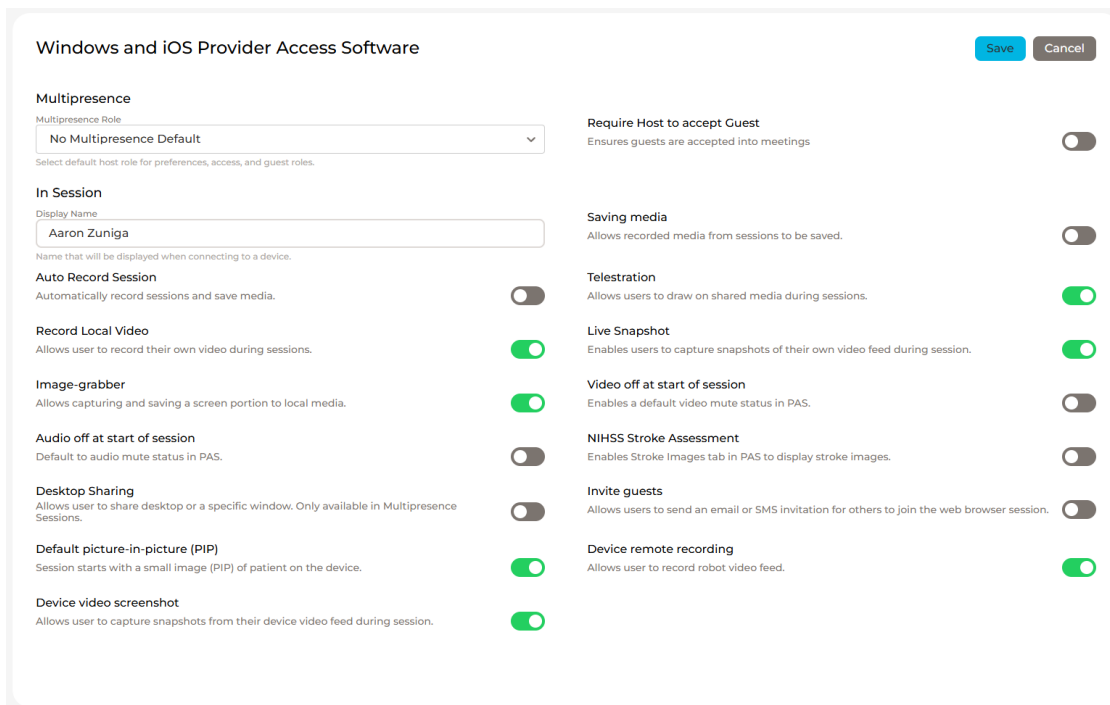
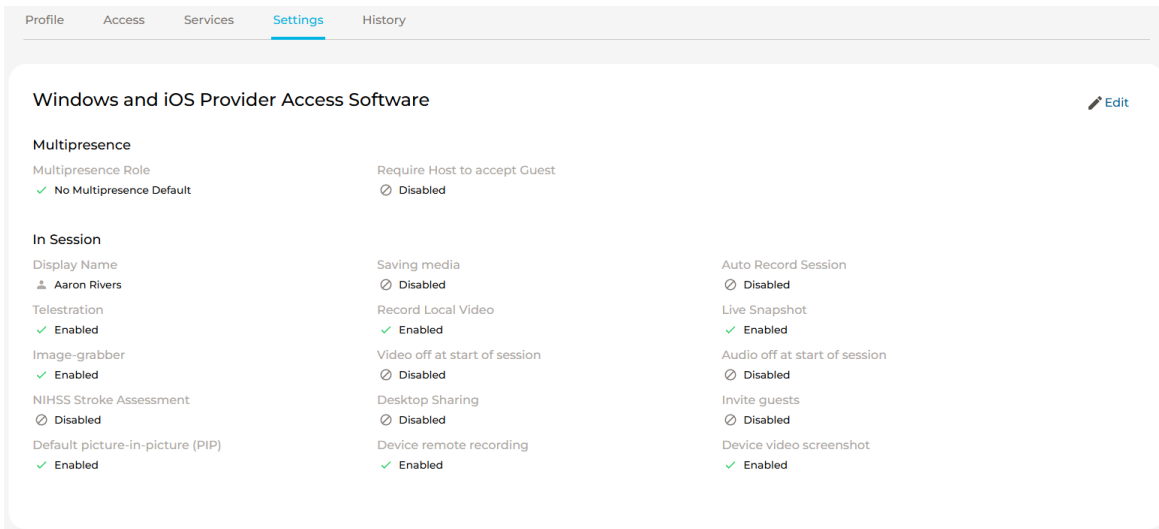


## Settings

The Settings tab show the settings that the user has for Windows and iOS Provider Access Software. The settings can be updated, and in case that the user is not enabled for Provider Access Software it can be enabled.



The list of settings that are available in Fleet Access Manager are the following:

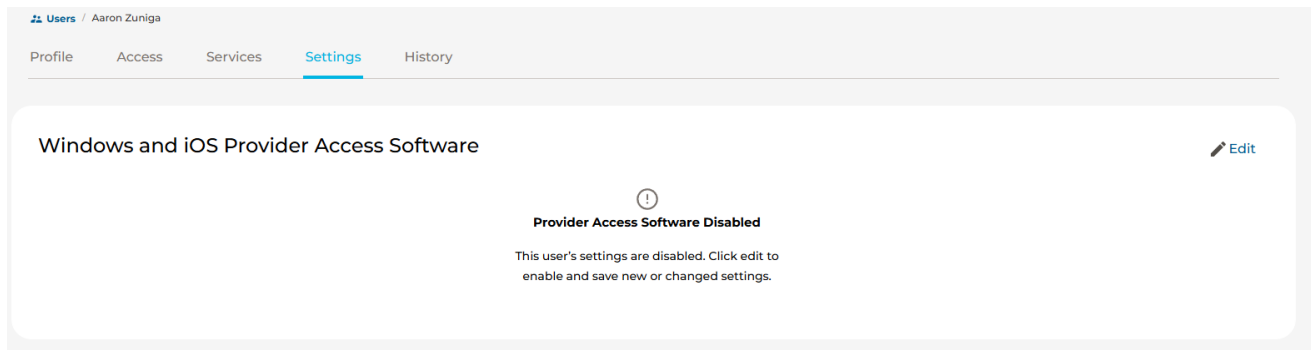


To update Provider Access Software Settings:

1. Click Edit
2. Update any number of settings that need to be changed
3. Click Save

To enable Provider Access Software Settings:

1. Click edit
2. Choose the settings or leave the default settings
3. Click Save



Note: When a user is not enabled for Windows or iOS Provider Access a message is displayed saying the user has Provider Access Software disabled.

## History

The History tab show changes done to the user the following changes are currently being displayed in the user history page

Changes to:

- First Name
- Last Name
- Email
- Enable/Disabled
- NPI
- Specialty
- Two Factor authentication



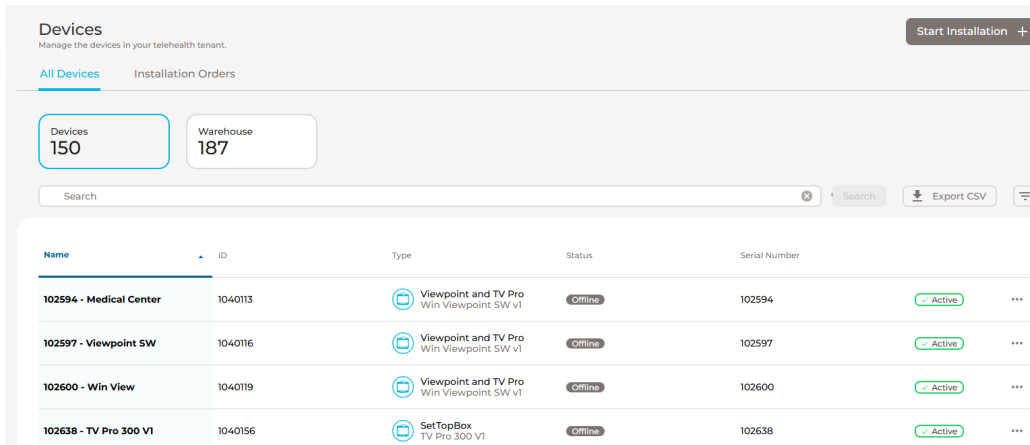
## Devices

Use the Devices page to view and edit Teladoc Health devices and configure user access for devices in your organization. You can sort the table by all five columns. If the device is inactive an inactive button in its row will be displayed.

Click the filter button (  ) to filter the table by

- active devices (the default)
- active and online
- active and busy
- active and offline
- deactivated
- all devices

Devices can be in use or in warehouse. Warehouse devices can be moved to a location to be used.



Column	Description
Name	The name of the device.
ID	The device's ID number
Type	The type of device. Devices are categorized by product type and within that category, there are the product sub- types. Product Type and Subtype names identify the software version that a device has.

Status	Whether the device is online, busy or offline.
Serial Number	The device's serial number
...	Click the ellipses for editing, access, history, device swap, move to storage

## Definitions

### Warehouse

Warehouse devices are associated with the Tenant but not available to be used, they can't be added to programs, services, locations or practices.

### Devices

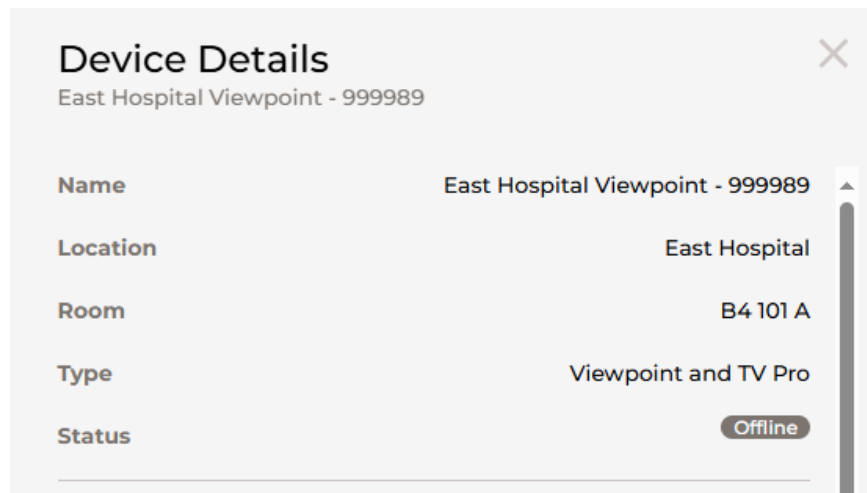
A telehealth device associated to a care location. The software that powers it is either installed by Teladoc Health or by a customer using a Teladoc Health Viewpoint license.

## Device Side Panel

Use the device side panel to view additional information about a device. The information in the side panel is

**General Information:** This section of the side panel shows general information about the device. Name, Location, Room, Type, Status

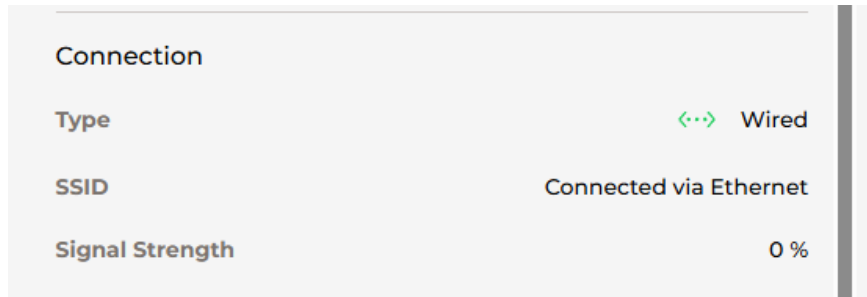
Column	Description
Name	The name of the device.
Room	The location room associated with the device
Type	The type of device. Devices are categorized by product type and within that category, there are the product sub- types. Product Type and Subtype names identify the software version that a device has.
Status	Whether the device is online, busy or offline.



**Connection:** This section of the side panel shows the connection information of the device. Connection Type, SSID, Signal Strength

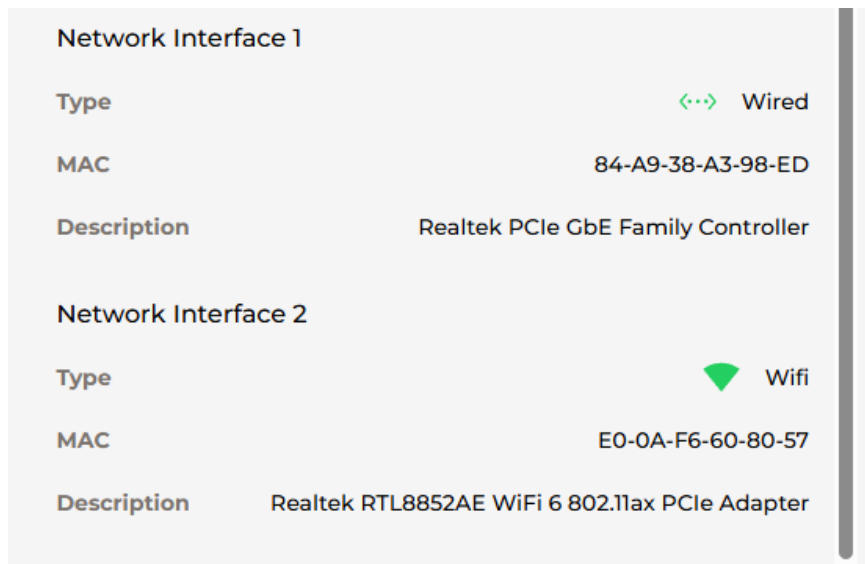
Column	Description
Type	The type of the network interface in use. Possible values are Wired, Mobile, and Wifi
SSID,	The SSID of the network in use. If the connection type is wired it shows "Connected via Ethernet"

Signal Strength	The signal strength of the network in use. If the connection type is wired it shows "0%"
-----------------	--



Network Interfaces: This section of the side panel shows the available network interfaces the device has. Each network adapter shows

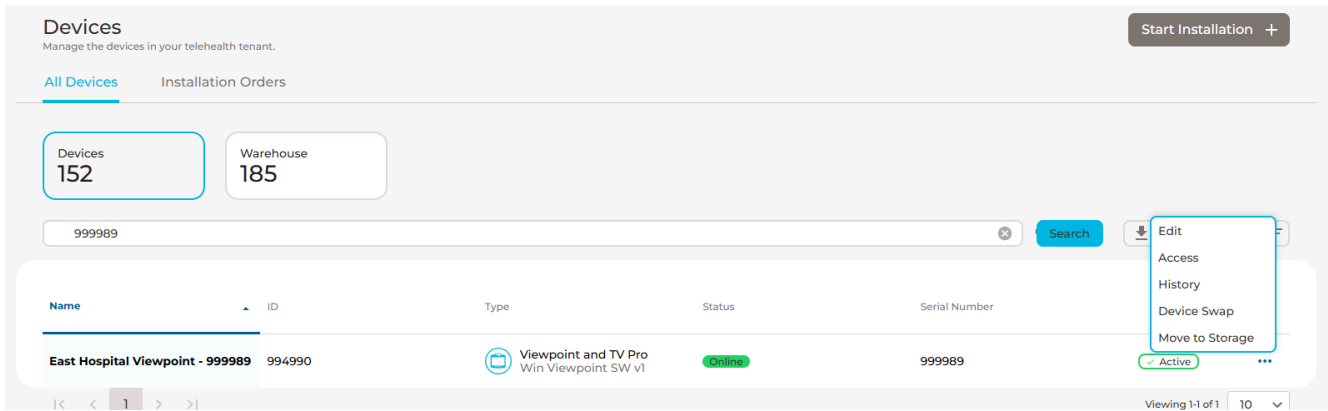
Column	Description
Type	The type of the network adapter. Possible values are Wired, Mobile, and Wifi
MAC,	The MAC address of the network adapter
Description	The network adapter device description



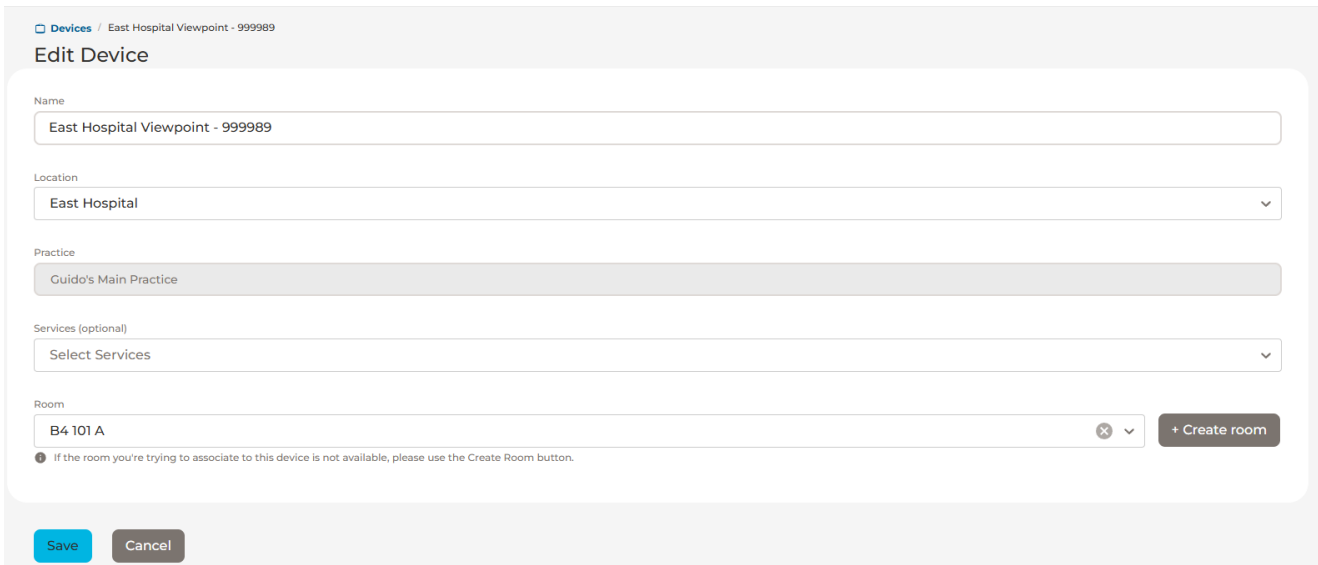


## Edit Devices

1. Select the device you want to edit.
2. Click the three horizontal dots in its row and select **Edit**.



The following will be displayed.



1. The device name can be updated, if needed.
2. The Location can be updated, if needed
  - a. Moving a device to a new location may move it to a different practice.
3. Update the devices services, if needed
4. Choose a room for the device, if needed
  - a. A new room can be created in the Location if needed by clicking the Create Room button, a side panel will be shown to add a new room to the location

### Create Room ✕

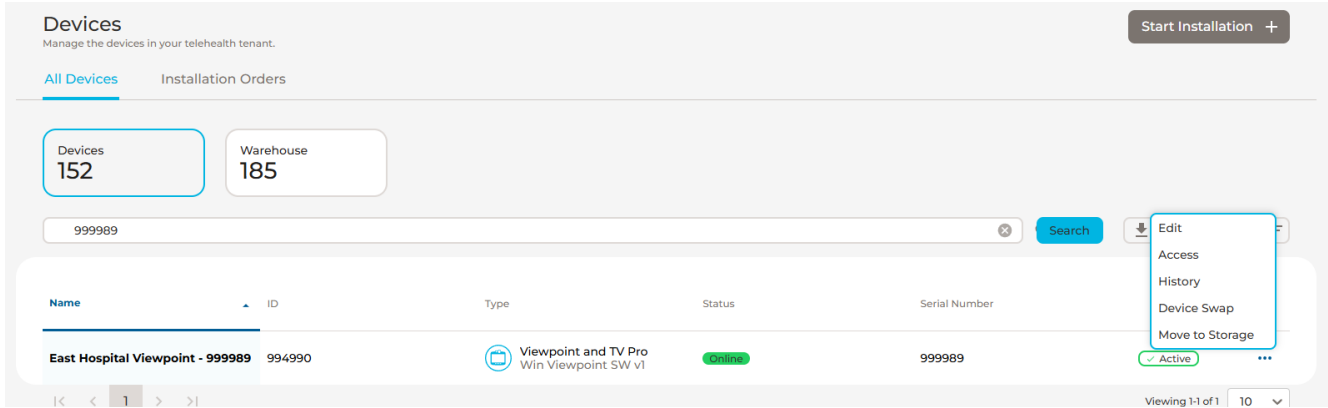
Location

Room name

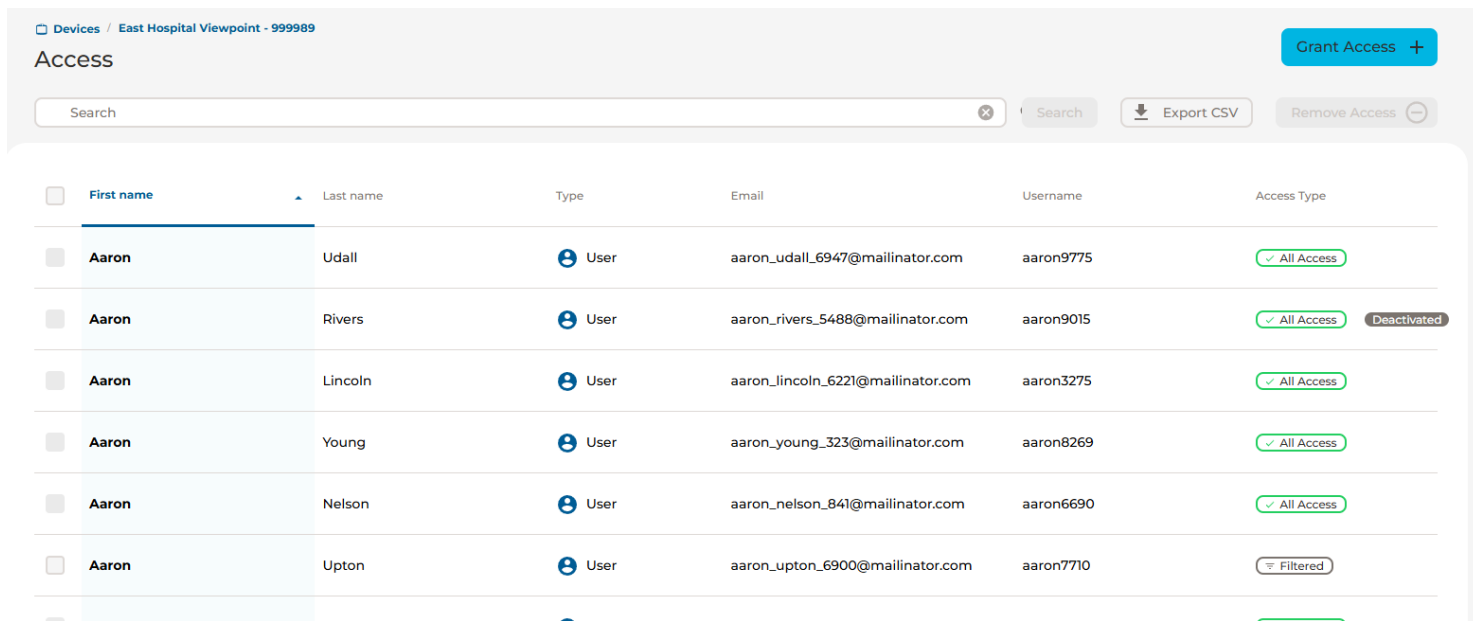
## Viewing Device Access

Fleet access manager offer an access page to see who can connect to a device you own.

1. Select the device you want to view its users.
2. Click the three horizontal dots in its row and select **Access**



The following will be displayed.

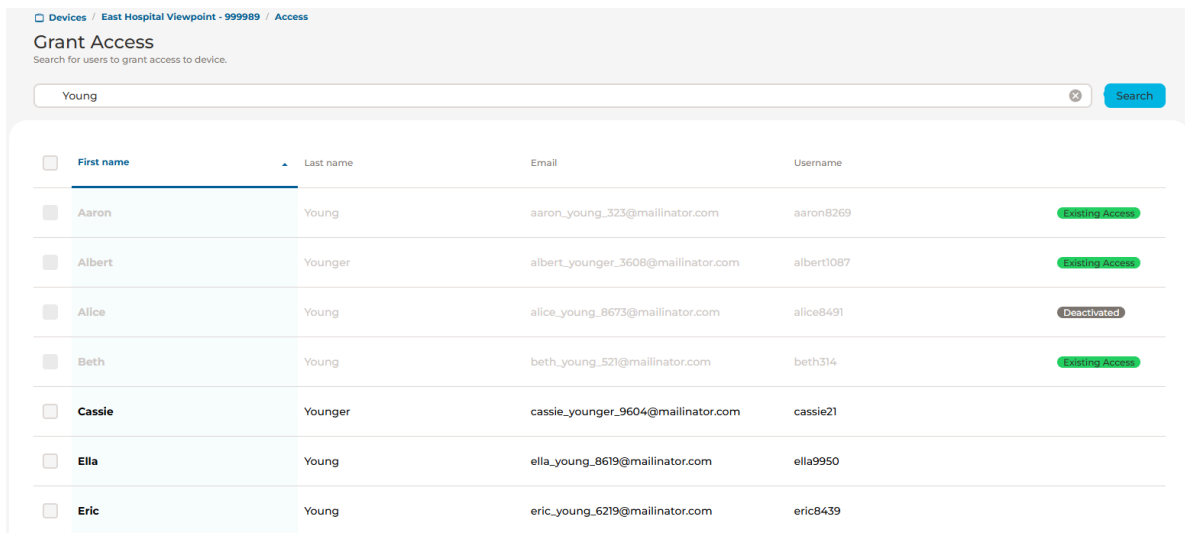


## Adding Individual User Access to a Device

Fleet Access Manager offers a way to add individual access to a device from within the device access page

Note: For managing access in groups see the “All Access” programs in the program section

1. Select the device you want to add users.
2. Click the three horizontal dots in its row and select **Access** or click anywhere in the device's row.
3. Click **Grant Access**.
4. Enter the name of the users you want to add in the search window.
5. Click **Search**.



1. Select the checkbox next to **First name** to select all users or select one or more users. Users with existing access will be grayed out.
2. Click **Grant Access to N Users** at the bottom of the table
3. Click **Grant Access to Users** to confirm the access on the modal displaying the access to be granted

**Review Selected Users**



	First name	Last name	Email	Username
	Cassie	Younger	cassie_younger_9604...	cassie21
	Ella	Young	ella_young_8619@m...	ella9950

**Grant Access to 2 Users**

Cancel

## Removing Device Users

1. Select the device from which you want to remove users.
2. Click the three horizontal dots in its row and select **Access** or click anywhere in the device's row.
3. Select the checkbox next to First Name at the top of the table to remove all users or select one or more users.

Devices / East Hospital Viewpoint - 999989

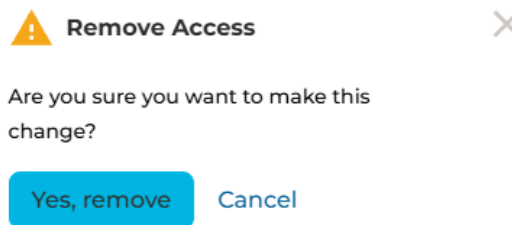
Access

Young  Search

<input type="checkbox"/>	First name	Last name	Type	Email	Username	Access Type
<input type="checkbox"/>	Aaron	Young	User	aaron_young_323@mailinator.com	aaron8269	All Access
<input type="checkbox"/>	Albert	Younger	User	albert_younger_3608@mailinator.com	albert1087	All Access
<input type="checkbox"/>	Alice	Young	User	alice_young_8673@mailinator.com	alice8491	All Access <span>Deactivated</span>
<input type="checkbox"/>	Beth	Young	User	beth_young_521@mailinator.com	beth314	All Access
<input checked="" type="checkbox"/>	Cassie	Younger	User	cassie_younger_9604@mailinator.com	cassie21	Filtered
<input checked="" type="checkbox"/>	Ella	Young	User	ella_young_8619@mailinator.com	ella9950	Filtered

Viewing 1-6 of 6 10

4. Click **Remove Access**. The following will be displayed.

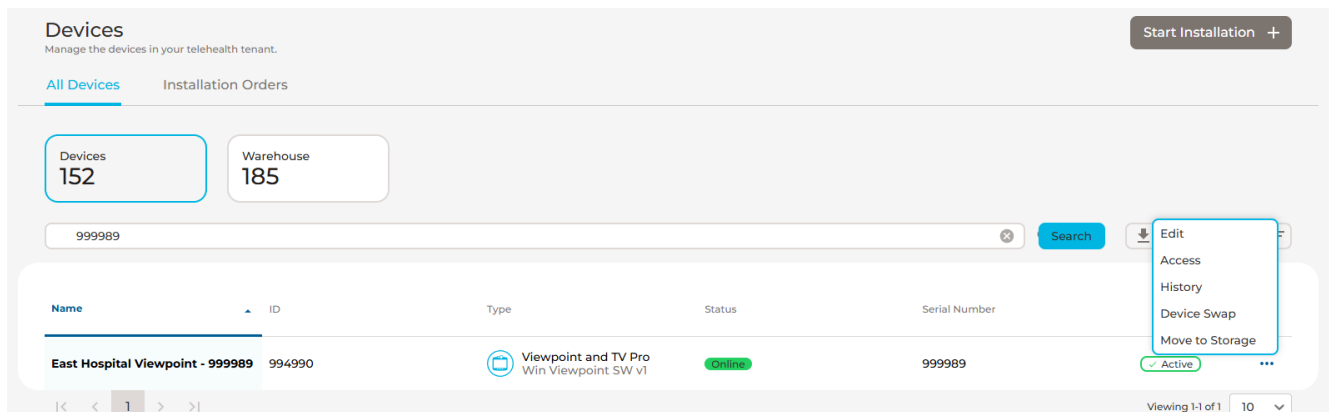


5. Click **Remove**.

## Device Swap

The device swap feature allows you to replace an active device with one from the warehouse while automatically transferring all configurations. When a device needs replacement, instead of manually setting up the new device's Location, Programs, Access, Practice, and Services, you can perform a device swap. This process moves the old device to warehouse status while the replacement device inherits all settings and configurations from the replaced device, streamlining the replacement process and ensuring continuity of service. Select the device you want to view its history.

1. Select the device you want to swap
2. Click the three horizontal dots in its row and select **Swap**



The screenshot shows the 'Devices' management interface. At the top, there are two summary boxes: 'Devices 152' and 'Warehouse 185'. Below these is a search bar with the text '999989' and a 'Search' button. A table lists the devices with columns for Name, ID, Type, Status, and Serial Number. One device is highlighted: 'East Hospital Viewpoint - 999989' with ID '994990', Type 'Viewpoint and TV Pro Win Viewpoint SW v1', Status 'Online', and Serial Number '999989'. A dropdown menu is open for this device, showing options: 'Edit', 'Access', 'History', 'Device Swap', and 'Move to Storage'. The 'Device Swap' option is highlighted. At the bottom right, it says 'Viewing 1 of 1' and '10'.

3. Choose the device you want to swap the selected device with

### Swap Device ✕

Swapping a device will replace the active device with one chosen from storage. This action will reassign the location, practice and services, and transfer all access to the new device. The current device will no longer be active and will be moved to storage.

Current Device

999989 - Win Viewpoint SW v1

Select replacement device

102946 - Win Viewpoint SW v1 ▾

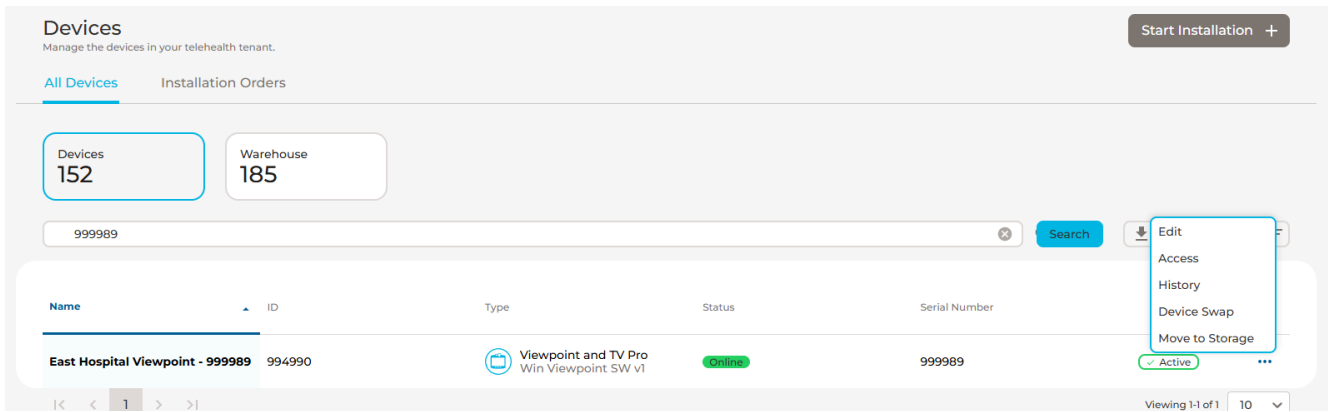
Cancel Submit



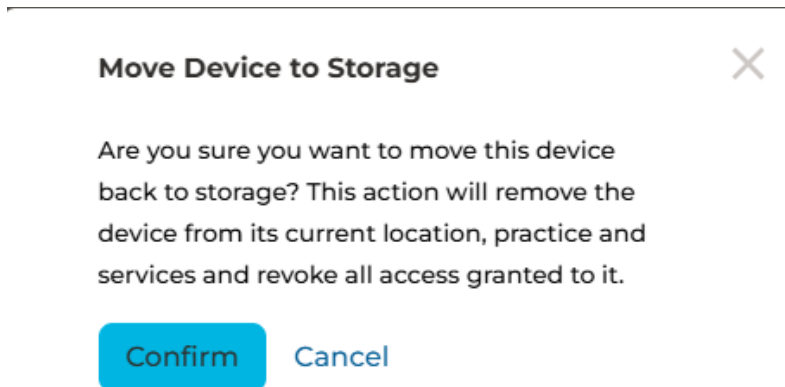
### Move a Device to a Warehouse status

Devices removed from active deployment can be moved to warehouse status, which prevents them from being added to programs, receiving individual access, or being used in Practices or Services. While in warehouse, devices remain inactive until they are redeployed to a new location, where they can be fully reconfigured for their new purpose. Select the device you want to swap

1. Click the three horizontal dots in its row and select **Move to Storage**

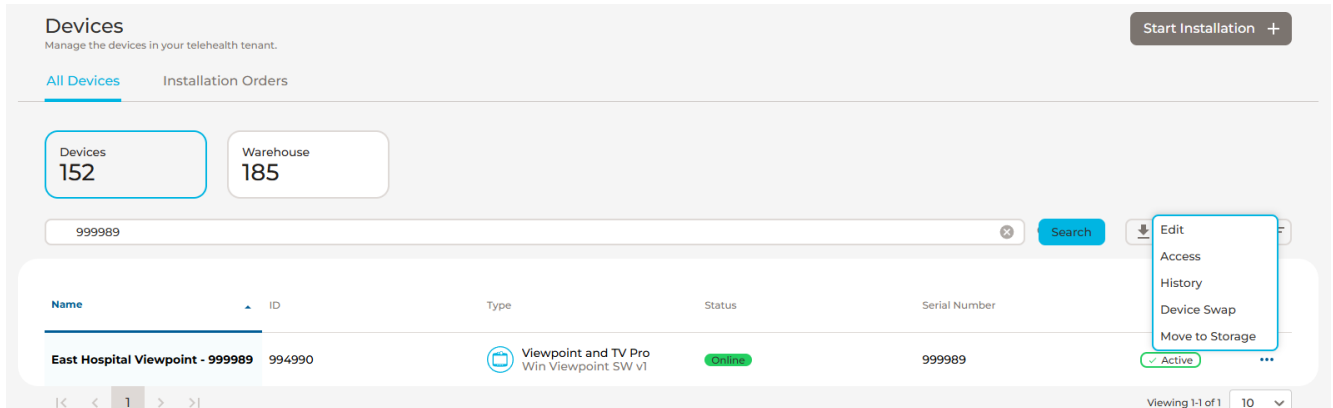


2. Confirm that the device will be moved to your warehouse devices

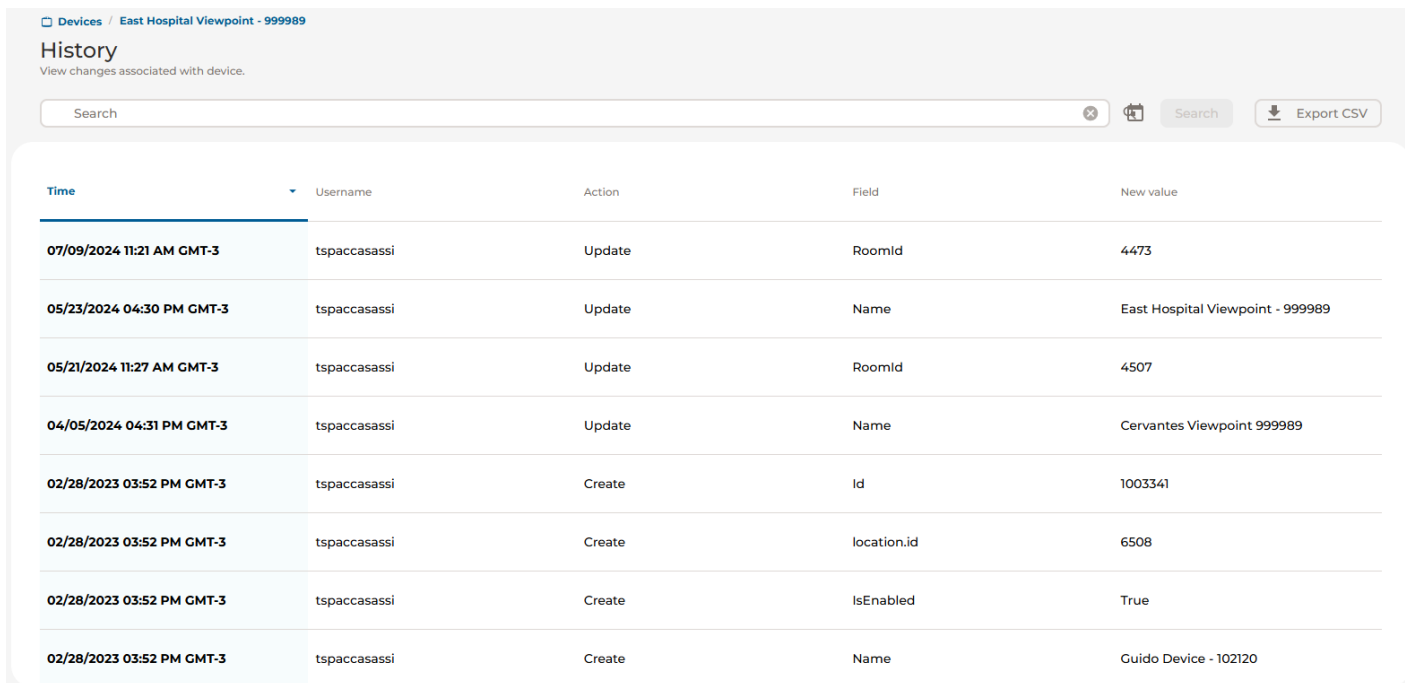


## Device History

1. Select the device you want to view its history.
2. Click the three horizontal dots in its row and select History or click anywhere in the device's row.



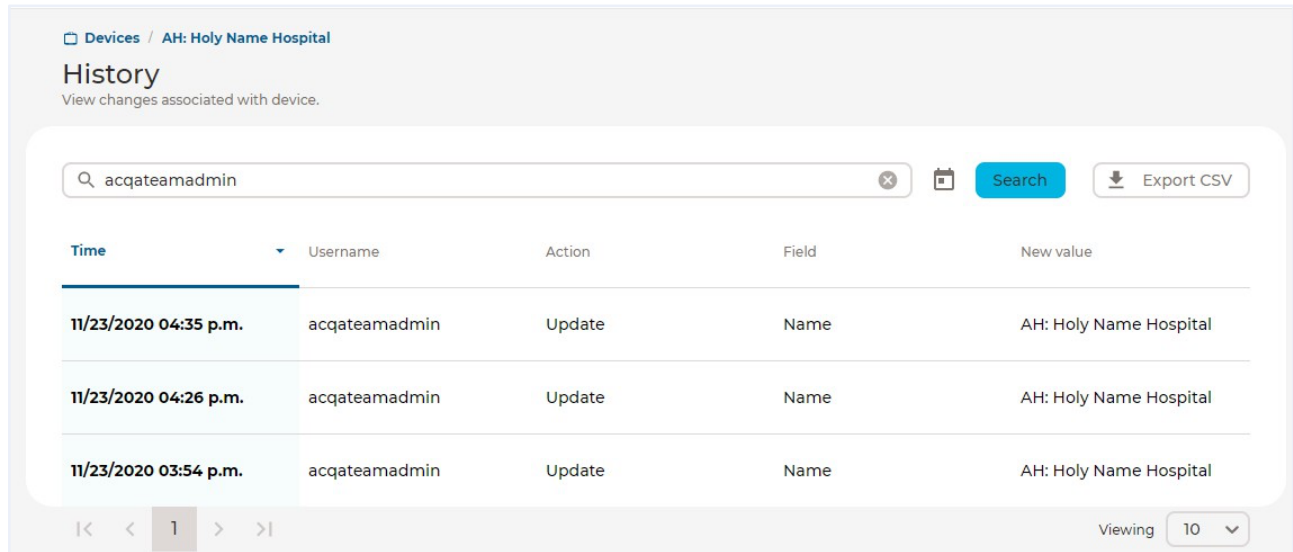
The following will be displayed. You can sort this table by any column except for New Value



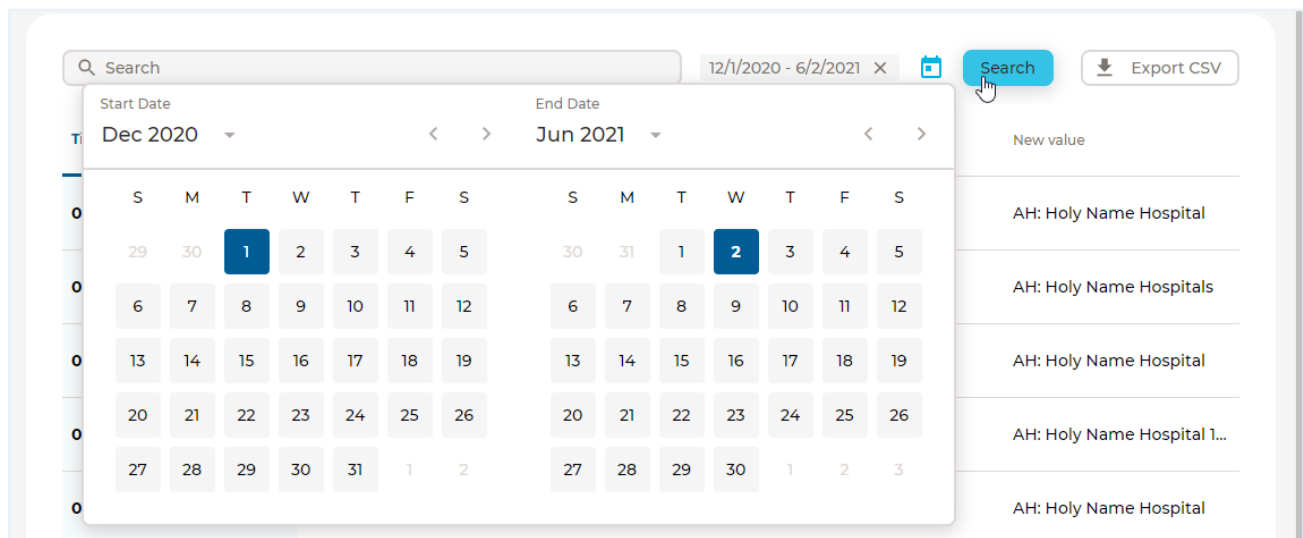
Column	Description
Time	The local day and time the device field was changed.
Username	The name of the user who changed the device field.
Action	The modification type the user performed, which can be Create or Update.

Field	The field the user modified.
New value	The device field's new value.

1. You can filter the results by entering a username, action, field, or value in the search bar. Click the X to clear your results.



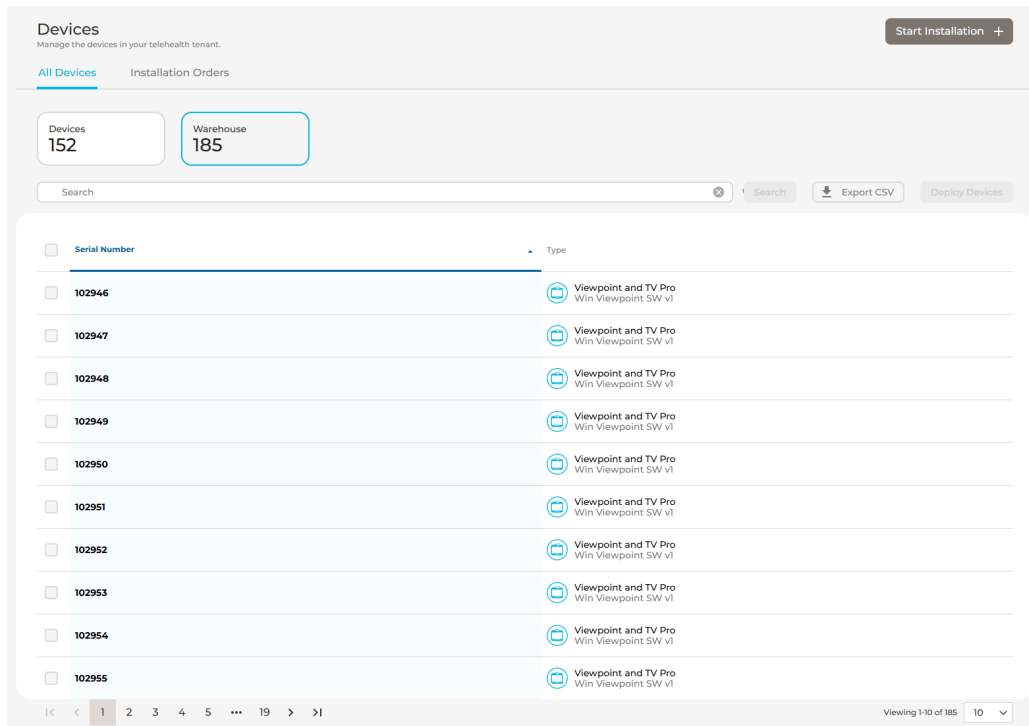
2. You can select a date range by clicking the date picker (📅), then selecting the start and end dates, and then clicking **Search**.



Click the X to clear your results.

## Warehouse Devices

Devices in warehouse status, are prevented from being added to programs, receiving individual access, or being used in Practices or Services. While in warehouse, devices remain inactive until they are deployed to a new location, where they can be fully reconfigured for their new purpose. Devices in warehouse can also be swapped in to replace a device



Column	Description
Serial Number	The Serial Number of the device.
Type	The type of device. Devices are categorized by product type and within that category, there are the product sub- types. Product Type and Subtype names identify the software version that a device has.

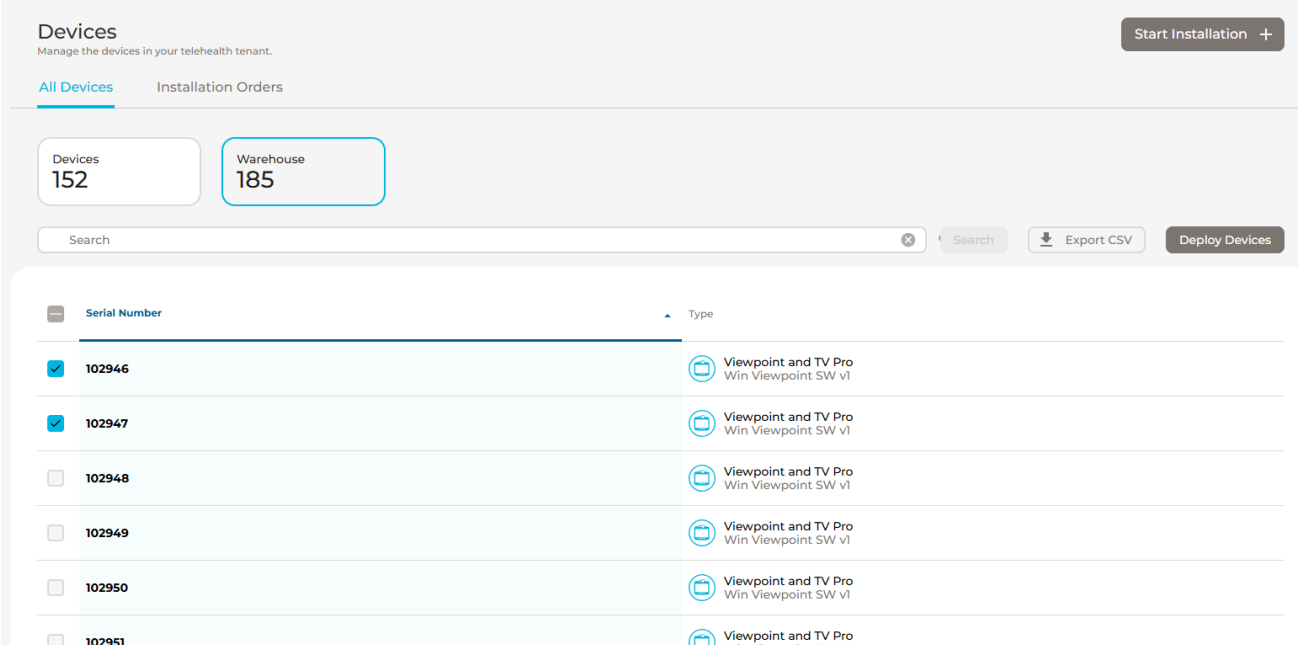
## Deploying a Device

Fleet Access Manager offers two methods for device deployment. The first method is direct deployment, which is used when you have a specific device's serial number and know its intended location. This approach is ideal for precise, single-device installations.

The second method uses installation orders, which are better suited for deploying multiple devices when the serial numbers or exact room locations aren't known in advance. When creating an installation order, it initiates a workflow where the installation team can document the serial numbers and room locations as devices are installed. This flexible approach accommodates bulk deployments and allows for on-site decision-making about device placement.

### Deploying a device from the warehouse page

1. Select devices for deployment by checking the boxes next to their serial numbers.
2. Click the "Deploy Devices" button to begin the deployment process.



The screenshot shows the 'Devices' management interface. At the top, there are two summary boxes: 'Devices 152' and 'Warehouse 185'. Below these is a search bar and buttons for 'Search', 'Export CSV', and 'Deploy Devices'. The main table lists devices with the following data:

Serial Number	Type
<input checked="" type="checkbox"/> 102946	Viewpoint and TV Pro Win Viewpoint SW v1
<input checked="" type="checkbox"/> 102947	Viewpoint and TV Pro Win Viewpoint SW v1
<input type="checkbox"/> 102948	Viewpoint and TV Pro Win Viewpoint SW v1
<input type="checkbox"/> 102949	Viewpoint and TV Pro Win Viewpoint SW v1
<input type="checkbox"/> 102950	Viewpoint and TV Pro Win Viewpoint SW v1
<input type="checkbox"/> 102951	Viewpoint and TV Pro

3. Assign names to each device. Default name placeholders are provided but can be customized as needed.
4. Select the destination location for device deployment
5. (Optional) Assign devices to a specific organization. This selection determines which reports will include data from these devices

**Deploy Devices** [X]

Device Name  
Gont Device - 102946 [−]

Serial Number: 102946      Device SubType: Win Viewpoint SW v1

---

Device Name  
Gont Device - 102947 [−]

Serial Number: 102947      Device SubType: Win Viewpoint SW v1

**Total Devices: 2**

---

Location  
Gont Medical Center [v]

Organization (optional)  
Guido Division 3 [x] [v]

6. Click "Deploy" to complete the device relocation process.
7. The system will display the practice associated with the device's new location to confirm successful deployment.

**Devices** [X]

**i** The devices you chose have been successfully deployed. You may now choose a service for the group.

Practice  
Guido's Spoke 2

**i** To change the practice associated with this location please email [fleetops@teladohealth.com](mailto:fleetops@teladohealth.com).

Services (optional)  
Select service [v]

8. (Optional) Configure services for the deployed devices.
9. Click "Save" to finalize service selections.

### Deploying a device using an installation order

1. Go to the Installation Orders tab
2. Click Start Installation
3. Choose the amount of devices that will be installed in a locations. Can only be used for TV Pro 300 devices.
4. Choose the location
5. The practice associated with the location will be displayed. If there is no practice associated with the location please choose one
6. Choose the Programs that the devices will be a part of
7. Choose one or many email addresses of the people that will be installing the devices
8. Optional. Put any comment that you want, it will be displayed in the order history and in the email to the people that will install the devices.

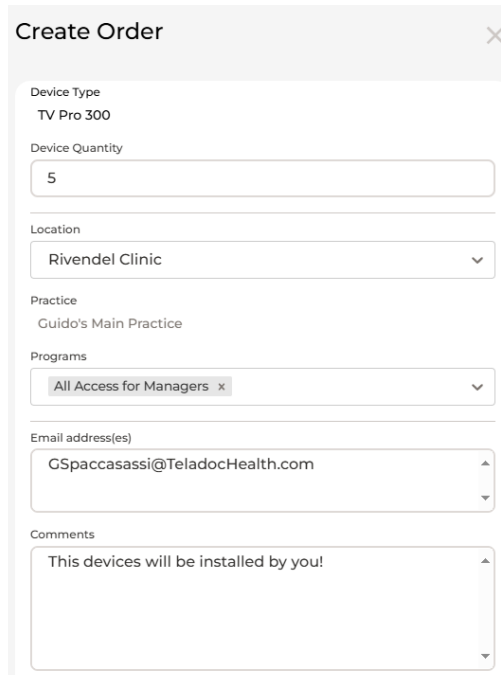
### Deploying Devices Using an Installation Order

1. Navigate to the Installation Orders tab.

The screenshot shows the 'Devices' management interface. At the top right, there is a 'Start Installation +' button. Below it, the 'Installation Orders' tab is selected. A summary section shows four status categories: Created (11), In Progress (2), Completed (3), and Closed (2). Below this is a search bar and an 'Export CSV' button. The main part of the interface is a table with the following columns: Status, Order Name, Created By, Location, Devices, and Creation Date.

Status	Order Name	Created By	Location	Devices	Creation Date
Created	Order BA5C79	tspaccasassi	East Hospital	0 of 10	5/22/2024
Created	Order B3E802	msandoval	Gont Medical Center	0 of 1	2/2/2024
Created	Order C1E8CA	msandoval	Gont Medical Center	0 of 1	2/2/2024
Created	Order 979542	tspaccasassi	Gont Medical Center	0 of 10	12/13/2023
Created	Order 0325C9	tspaccasassi	Main Hospital	0 of 20	12/7/2023

2. Click "Start Installation" to begin the process.



The screenshot shows a 'Create Order' dialog box with the following fields:

- Device Type:** TV Pro 300
- Device Quantity:** 5
- Location:** Rivendel Clinic
- Practice:** Guido's Main Practice
- Programs:** All Access for Managers x
- Email address(es):** GSpaccasassi@TeladocHealth.com
- Comments:** This devices will be installed by you!

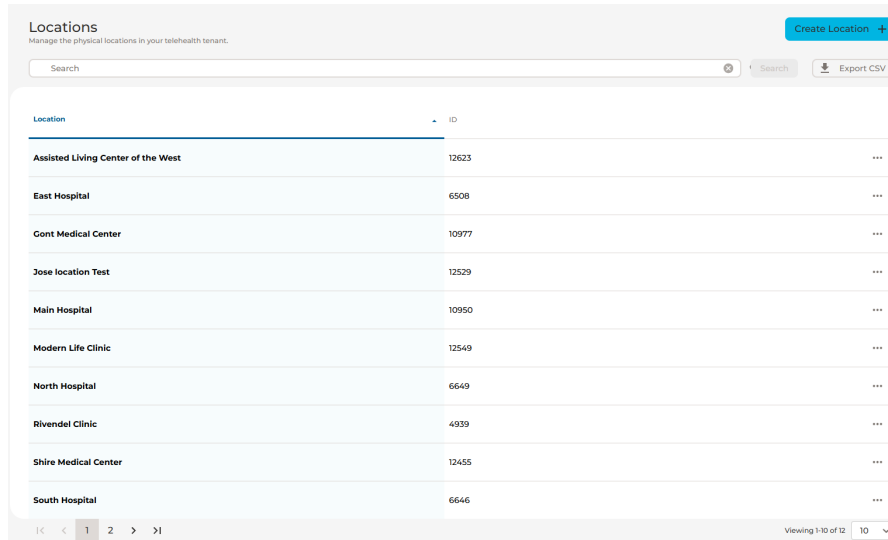
3. Specify the number of devices to be installed at the location. Note: This feature is only compatible with TV Pro 300 devices.
4. Select the destination location for installation.
5. Verify the practice associated with the location. If no practice is currently associated, select one from the available options.
6. Select the programs that will be assigned to these devices.
7. Enter the email addresses of the installation team members who will perform the device setup.
8. (Optional) Add comments to provide additional context or instructions. These comments will appear in both the order history and the installation team's email notification.

It can be tracked in the Installation Orders tab. For more information on orders see Annex 1



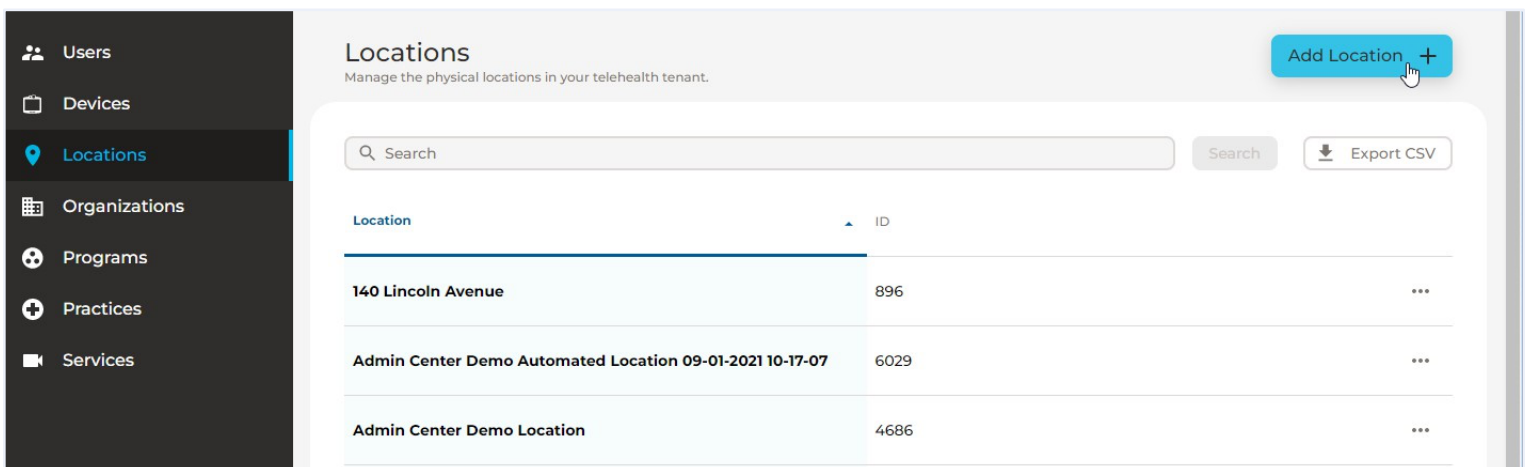
## Locations

A location is a physical building where care is delivered. Use the Locations page to view its history, edit, add, and remove locations from your organization. You can sort the table by either column.



### Adding Locations

1. Click **Locations** in the left-hand navigation bar.
2. Click **Add Location**.



The following will be displayed.

**Locations**

### Add a Location

Location Name

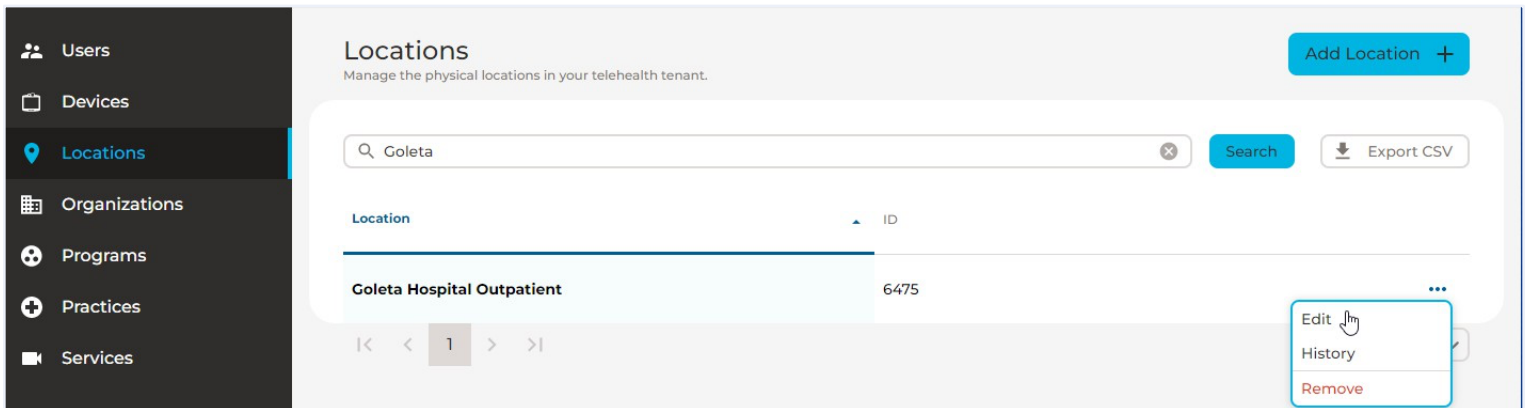
Organization

Practices

1. Enter the location's name.
2. Select an organization from the Organization dropdown.
3. Select a Practice from the Practices dropdown.
4. Click **Save**.

### Edit Locations

1. Select the location you want to edit.
2. Click the three horizontal dots in its row and select **Edit**.



The following will be displayed.

Assisted Living Center of the West ✎ Edit

Practice  
Guido's Main Practice

**Rooms**

Search  ✕ 🔍 Add Rooms +

---

Room Name

---

**List of rooms is empty**  
There are no rooms to show. Click on 'Add Rooms' to create them.

## Name and Practice

Assisted Living Center of the West Save Cancel

Location

Practice

🔗 To change the practice associated with this location please email [fleetops@teladohealth.com](mailto:fleetops@teladohealth.com).

1. Click Edit
2. Update the Location Name
3. If the Location is not associated with a Practice it can be associated with one
4. Click **Save**.

**Note:** When a Location is associated with a Practice, all devices in that Location become available in that Practice. To change a Location's associated Practice, please email Fleet Operations ([fleetops@teladohealth.com](mailto:fleetops@teladohealth.com)). Keep in mind that all devices will be transferred to the new Practice.

### Location Rooms

Certain features like Virtual Sitter require rooms to be defined in Locations before they can be associated with devices.

#### Create Single Rooms

1. Click "Add Rooms"
2. Enter the room name
3. Click "Add another room" to create additional single rooms

#### Create Room Ranges

1. Click "Add Rooms"
2. Click "Room Range"
3. Enter:
  - a. Prefix (optional)
  - b. Start room number
  - c. End room number
  - d. Suffix (optional)

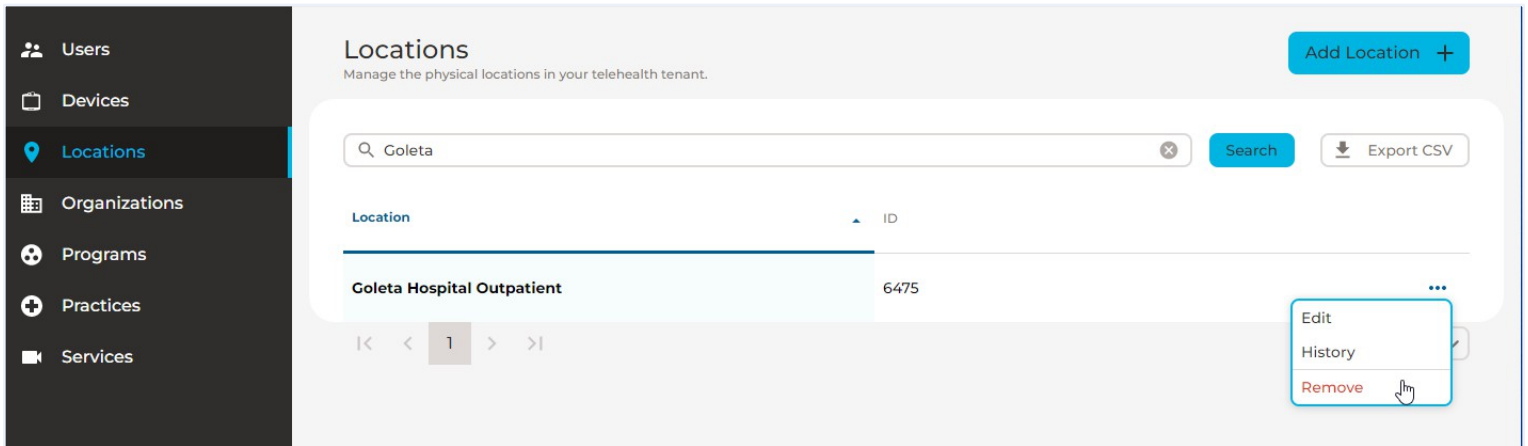
Note: Room ranges will generate rooms for every number between start and end (inclusive). Each room name will combine the prefix + room number + suffix (e.g., West 1A, West 2A, etc.)

Once created the rooms are displayed in the Location

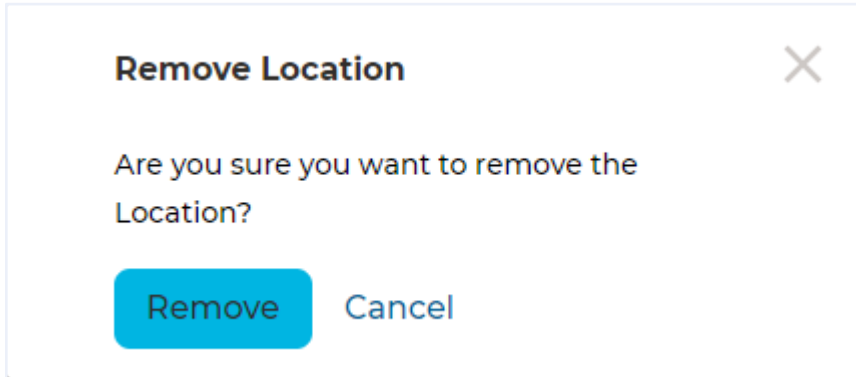
Room Name
West 1 A
West 2 A
West 3 A
West 4 A
West 5 A
West 6 A
West 7 A
West 8 A
West 9 A
West 10 A

### Remove Locations

1. Select the location you want to remove.
2. Click the three horizontal dots in its row and select **Remove**.

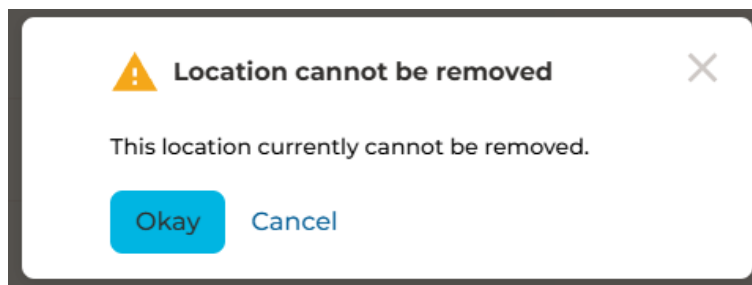


The following will be displayed.



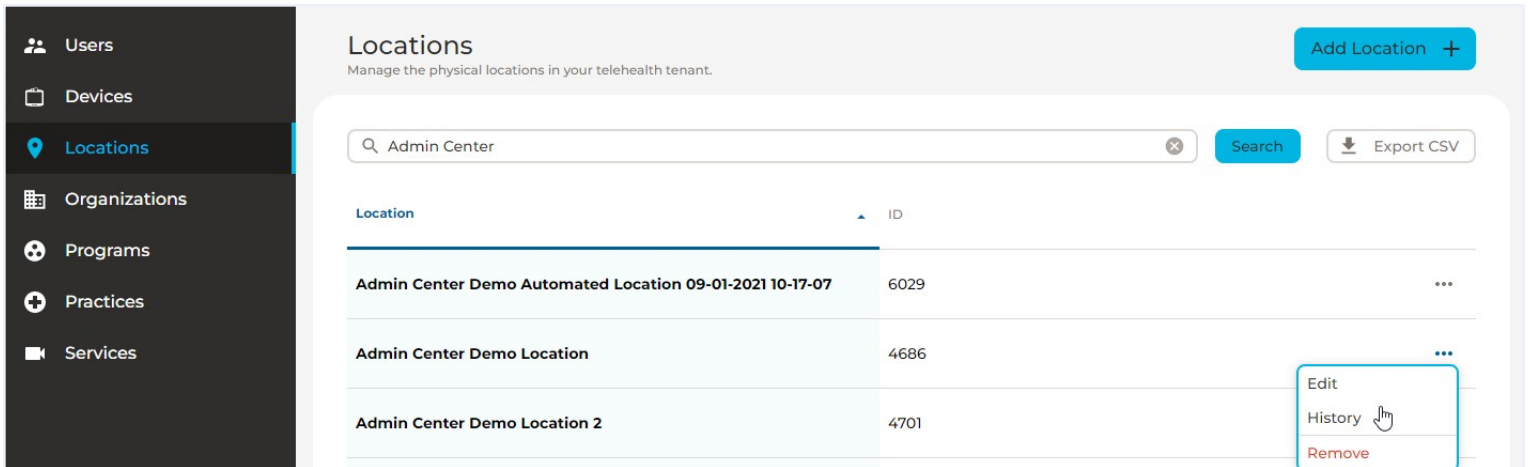
3. Click **Remove**.

Note: Locations cannot be removed if they have deployed devices or associated access rules. If you need to remove such a location, please contact Fleet Operations ([fleetops@teladochealth.com](mailto:fleetops@teladochealth.com)) or Support for assistance.

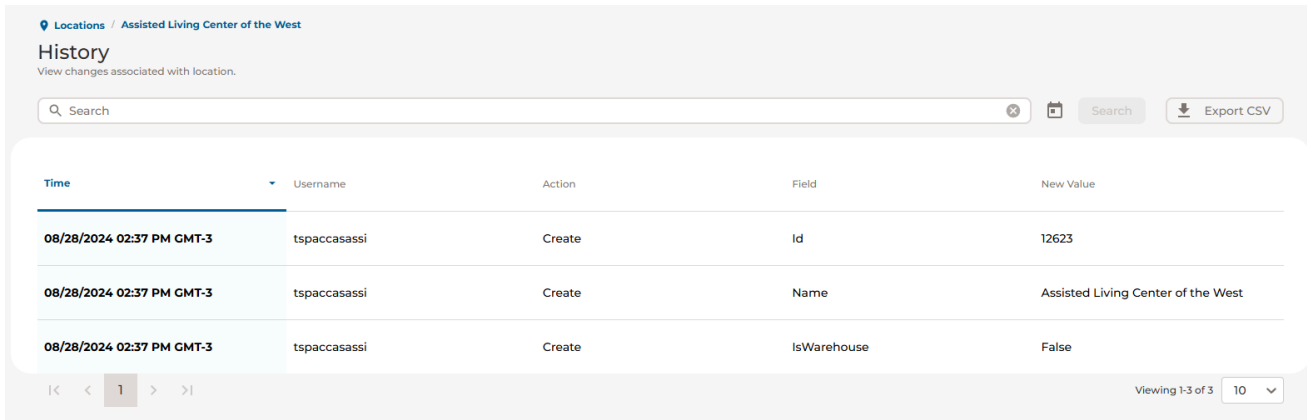


## Location History

1. Select the location you want to view its history.
2. Click the three horizontal dots in its row and select **History** or click anywhere in the location's row.



The following will be displayed. You can sort this table by any column except for New Value.



Column	Description
Time	The local day and time the device field was changed.
Username	The name of the user who changed the device field.
Action	The modification type the user performed, which can be Create or Update.
Field	The field the user modified.
New value	The device field's new value.

3. You can filter the results by entering a username, action, field, or value in the search bar. Click the X to clear your results.

Locations / Admin Center Demo Location

### History

View changes associated with location.

Search: Id [X] [Date Picker] [Search] [Export CSV]

Time	Username	Action	Field	New Value
10/28/2020 11:33 p.m.	aguerra	Create	Id	4686

Viewing 10

4. You can select a date range by clicking the date picker (📅), then selecting the start and end dates, and then clicking **Search**.

Search: Search [12/1/2020 - 6/2/2021] [X] [Date Picker] [Search] [Export CSV]

Start Date: Dec 2020 | End Date: Jun 2021

Selected dates: Dec 1, Jun 2

New value

- AH: Holy Name Hospital
- AH: Holy Name Hospitals
- AH: Holy Name Hospital
- AH: Holy Name Hospital 1...
- AH: Holy Name Hospital

Click the X to clear your results.



## Organizations

An Organization is the Legal/Corporate entity representing a healthcare organization (HCO). Organizations are only associated to one Tenant. Use the Organizations page to view the organizations in your telehealth program. You can sort the table by the Organization column.

**Search for one or more organizations.**

**Click here to create a CSV report of the current page.**

**Organizations**  
Manage the organizations in your telehealth tenant.

Search [ ] Search [ ] Export CSV [ ]

Organization	ID
Admin Center Demo	fddfe1ff-fcc0-4cf0-838e-c7c2d0e1253c
Admin Center Demo Account 3	711b60a0-1971-44b9-a419-f8487b003dfc
Admin Center QA Account 1 - Child 1	898b23ed-bafb-423d-99d2-4a29b38ee665

## Programs

Use the Programs page to display all Teladoc Health programs in your Tenant. You can sort the table in standard or reverse alphabetical order.

### Programs

Manage the programs in your telehealth tenant.

Add Program +

Search

 Export CSV

Program Name	Type	Access Type	
All Access for Managers	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
All Emergent Devices	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Behavior Health 1	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Clinic Providers	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Dermatology	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Division 4 Providers	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Dummy	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Group Access for Administrators	Administrative	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Southwest Clinic Doctors	Unknown	<span style="border: 1px solid #28a745; border-radius: 4px; padding: 2px;">✓ All Access</span>	⋮
Southwest Hospitals Program	Administrative	<span style="border: 1px solid #6c757d; border-radius: 4px; padding: 2px;">Filtered</span>	⋮

⏪ <
1
2
> ⏩

Viewing 1-10 of 11
 10

Column	Description
Name	Your program name
Type	The type of program
Access Type	The type of device access the program uses, Filtered or All Access.
⋮ ⋮ ⋮	Click the ellipses to edit. In Filtered Programs, Access Maps can be downloaded

## Access Types and Use-Cases

There are two types of access control programs to support your organization's needs: **All Access Programs** and **Filtered Programs**. Read below to learn more and make the best choice for your Program.

### All Access Programs

#### All Access Programs

All Access Programs are designed for simplified, comprehensive access control. When you add a user or a device to an All Access Program, it's automatically given access to all corresponding devices or users within that program.

1. **Adding a User:** Instantly grants the user access to all devices associated with that All Access Program.
2. **Adding a Device:** All users in the program are granted immediate access to the newly added device.
3. **Removing a User or Device:** Access will be revoked for that specific program, but it will remain intact if granted by another program.

It works best for

- Environments where bulk access is required.
- Situations that don't demand fine-grained access controls.

#### Filtered Programs

Filtered Programs offer a more tailored access control experience. In this model, access is granted at the user-device level, allowing for highly specific access configurations.

1. **User-Device Specific Access:** Each user-device pairing must be explicitly defined.
2. **Adding a User:** Adding a User doesn't grant access, Access is managed in the User's Access page
3. **Adding a Device:** Adding a Device doesn't grant access, Access is managed in the Device's Access page
4. **Removing a User or Device:** Removes the User or Device from the Program **without revoking access**.

It works best for

- Environments that require stringent, specific access controls.
- Complex setups where devices and users should be grouped into programs for data visualization

## Download Access Maps

For filtered programs, access maps can be downloaded. These maps provide graphical representations of the existing access relationships between users and devices. Access maps are provided as Excel files.

1. Click the three dots next to a Filtered Program.
2. Click "Access Map" to download the access map.

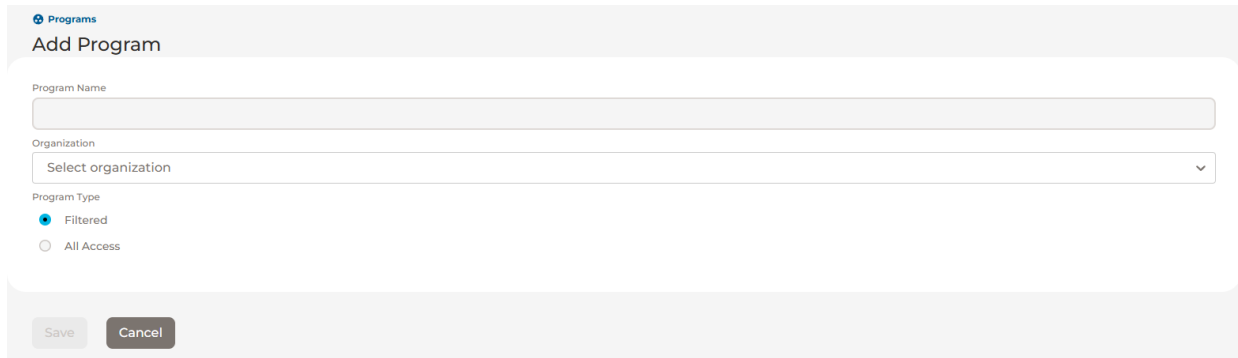
The screenshot shows an Excel spreadsheet with columns for User Full Name, Email, and Name. The data is organized into rows for each user and columns for each device. The cells are color-coded: green for access granted from the access page, blue for access granted by an All Access Program, and empty for no access granted.

User Full Name	Email	Win Viewpoint v1-103444	Win Viewpoint v1-103445	Win Viewpoint v1-103448	Win Viewpoint v1-103452	Win Viewpoint v1-103455	Win Viewpoint v1-103457	Win Viewpoint v1-103458
Adam Zimmer (adam3033)	adam_zimmer_6133@mailinator.com							
Adam Irving (adam8326)	adam_irving_144@mailinator.com							
Albert Hills (albert8957)	albert_hills_1298@mailinator.com							
Albert Evans (albert8822)	albert_evans_3807@mailinator.com							
Albert Ramsey (albert9203)	albert_ramsey_7837@mailinator.com							
Albert Clark (albert9417)	albert_clark_6436@mailinator.com							
Alex Xanders (alex2078)	alex_xanders_2403@mailinator.com							
Alice Russell (alice3490)	alice_russell_3769@mailinator.com							
Barry Baker (barry2969)	barry_baker_9326@mailinator.com							
Barry West (barry8604)	barry_west_4056@mailinator.com							
Becky Lee (becky5621)	becky_lee_9096@mailinator.com							
Becky Rowe (becky2209)	becky_rowe_749@mailinator.com							
Becky Gupta (becky1347)	becky_gupta_6120@mailinator.com							
Becky Xanders (becky2045)	becky_xanders_2466@mailinator.com							
Beth Walker (beth914)	beth_walker_4320@mailinator.com							
Beth Jenkins (beth1186)	beth_jenkins_3514@mailinator.com							
Beth Harper (beth756)	beth_harper_8239@mailinator.com							

Note: Green means that access is granted from the access page. Blue means that access is granted by an All Access Program. Empty means that no access is granted.

## How to Add Programs

1. Click **Programs** in the left navigation panel.
2. Click **Add Programs** in the upper right hand corner.

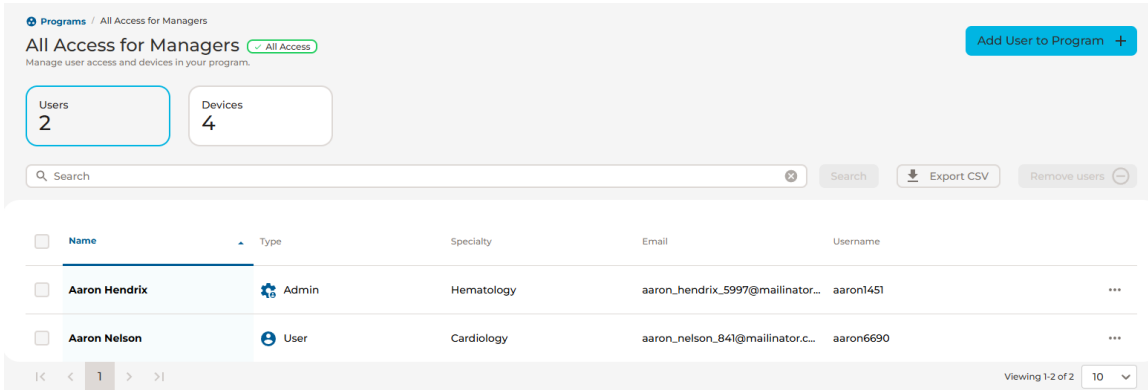


The screenshot shows a modal window titled "Add Program" with a "Programs" breadcrumb. It contains three main input fields: a text box for "Program Name", a dropdown menu for "Organization" with the text "Select organization", and a "Program Type" section with two radio buttons: "Filtered" (which is selected) and "All Access". At the bottom of the form are "Save" and "Cancel" buttons.

1. Enter the program's name.
2. Select the Organization from the dropdown.
3. Choose an Access Type:
  - a. Filtered
  - b. All Access

## Viewing Users or Devices in a Program

1. Click a program's row to view the program details.
2. Click on the "Users" tab to see the users associated with the program.
3. Click on the "Devices" tab to view the devices included in the program.



Programs / All Access for Managers

All Access for Managers ✓ All Access

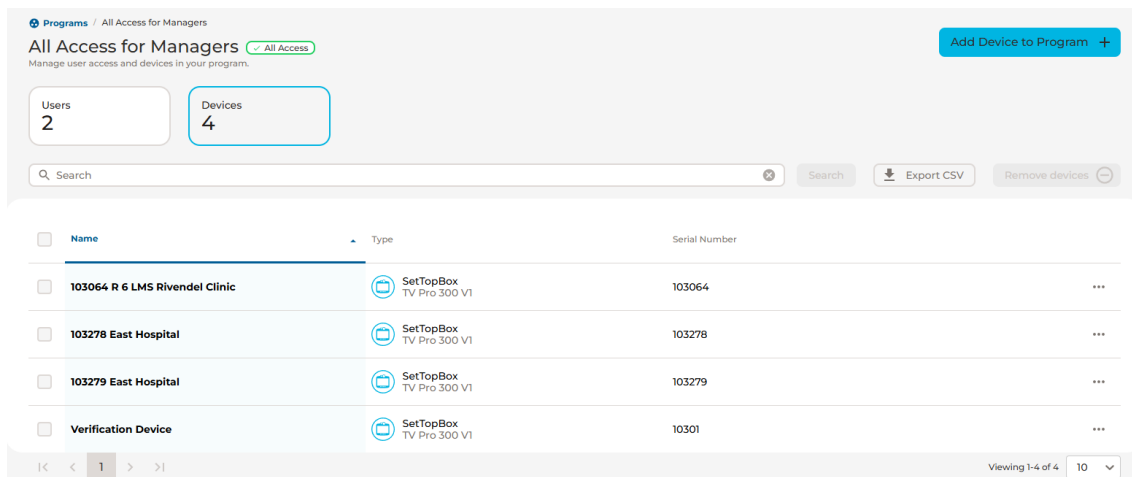
Manage user access and devices in your program.

Users: 2    Devices: 4

Search    Export CSV    Remove users

Name	Type	Specialty	Email	Username
<input type="checkbox"/> Aaron Hendrix	Admin	Hematology	aaron_hendrix_5997@mailinator...	aaron1451
<input type="checkbox"/> Aaron Nelson	User	Cardiology	aaron_nelson_841@mailinator.c...	aaron6690

Viewing 1-2 of 2



Programs / All Access for Managers

All Access for Managers ✓ All Access

Manage user access and devices in your program.

Users: 2    Devices: 4

Search    Export CSV    Remove devices

Name	Type	Serial Number
<input type="checkbox"/> 103064 R 6 LMS Rivendel Clinic	SetTopBox TV Pro 300 V1	103064
<input type="checkbox"/> 103278 East Hospital	SetTopBox TV Pro 300 V1	103278
<input type="checkbox"/> 103279 East Hospital	SetTopBox TV Pro 300 V1	103279
<input type="checkbox"/> Verification Device	SetTopBox TV Pro 300 V1	10301

Viewing 1-4 of 4

Note: Users who are in the program but are managed by another account will appear as "External" users; they can be removed.

## Removing Users or Devices

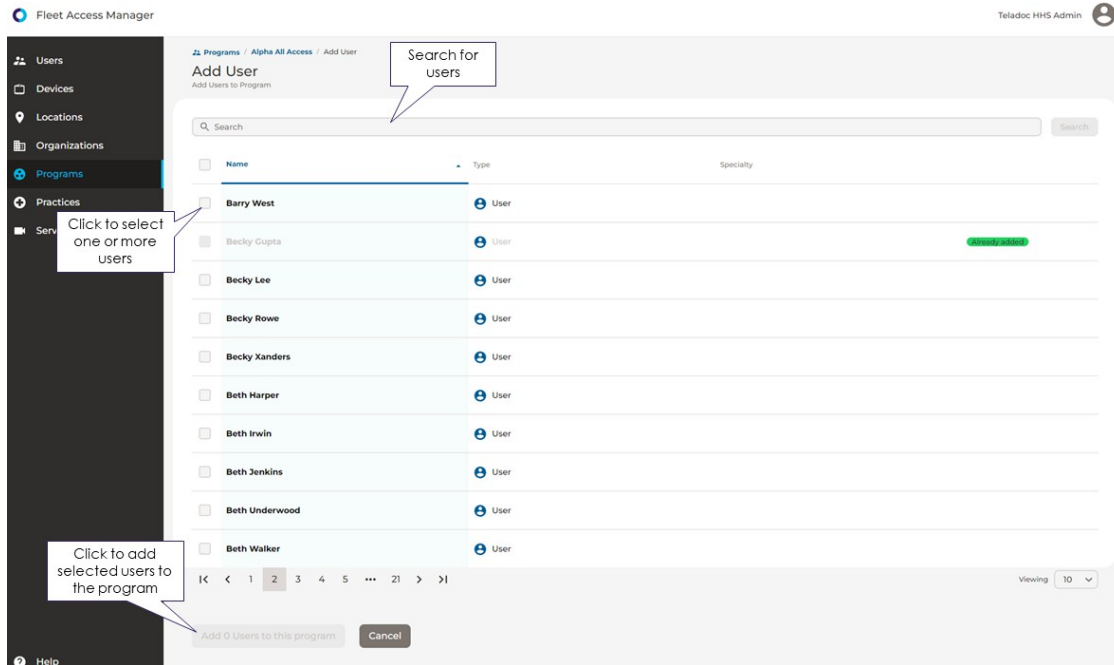
Users or devices can be removed from programs while viewing the program.

1. Check the box next to the users or devices you want to remove.
2. Click the button in the top-right corner that enables the removal of selected entities.

## Adding Users to a Program

1. Check the box next to the users you wish to add.
2. Click the button at the bottom of the page to add the selected users to the program.

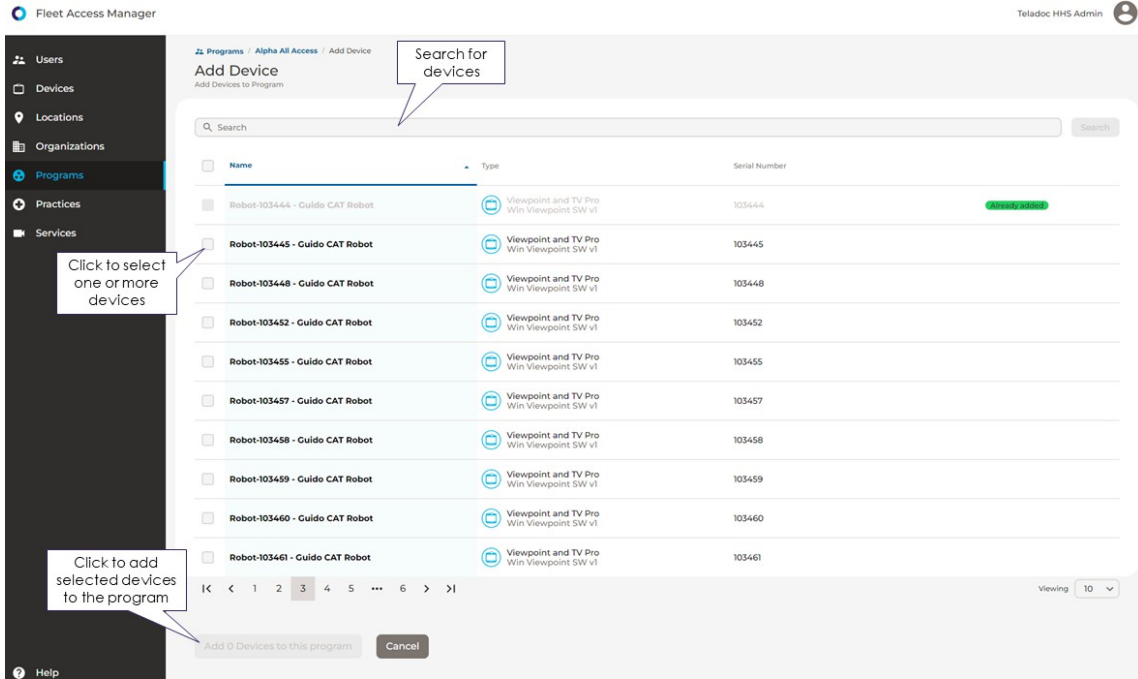
**Note:** Disabled users, as well as users who are already part of the program, are displayed here and are labeled.





## Adding Devices to a Program

1. Check the box next to the devices you wish to add.
2. Click the button at the bottom of the page to add the selected devices to the program.

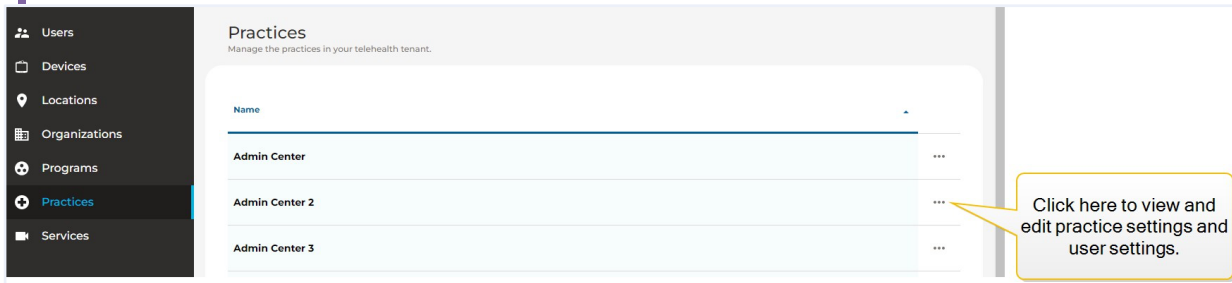


Note: Disabled devices, as well as devices that are already part of the program, are displayed here and are labeled.

## Practices

Use the Practices page to view and configure all the practices in a Tenant.

**Note:** The Practices page is not displayed if you have a Classic account. Contact your Teladoc Health representative if you have questions.

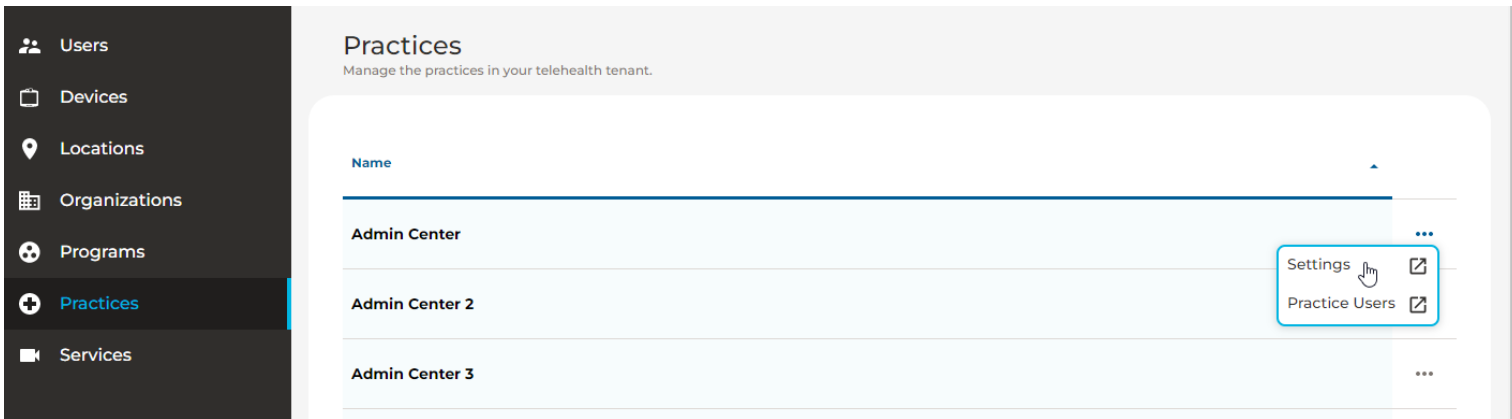


Click the three horizontal dots in a row and then select **Settings** or **Practice Users**. This will open the Practice Settings page or User Settings page for the practice in a new browser window.

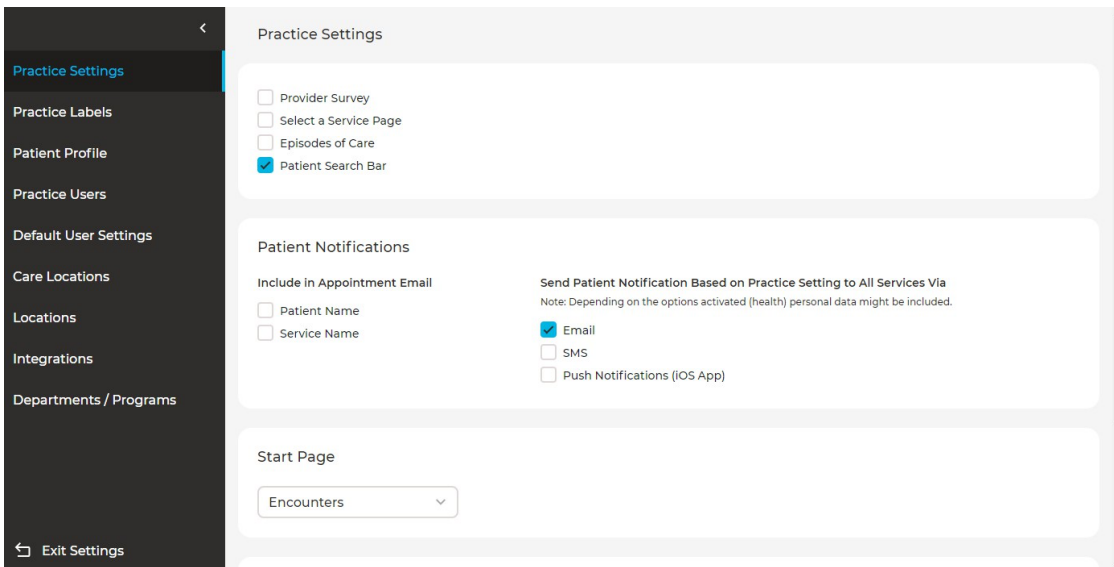
**Note:** See MA-20165 Teladoc Health Practice Admin User Guide for more information about configuring practices and see MA-20171 Teladoc Health Practitioner/Scheduler User Guide for more information about using Solo practices.

## Configuring Practice Settings

1. Click **Practices** in the left navigation panel.
2. Click the three horizontal dots for the practice and select **Settings**.



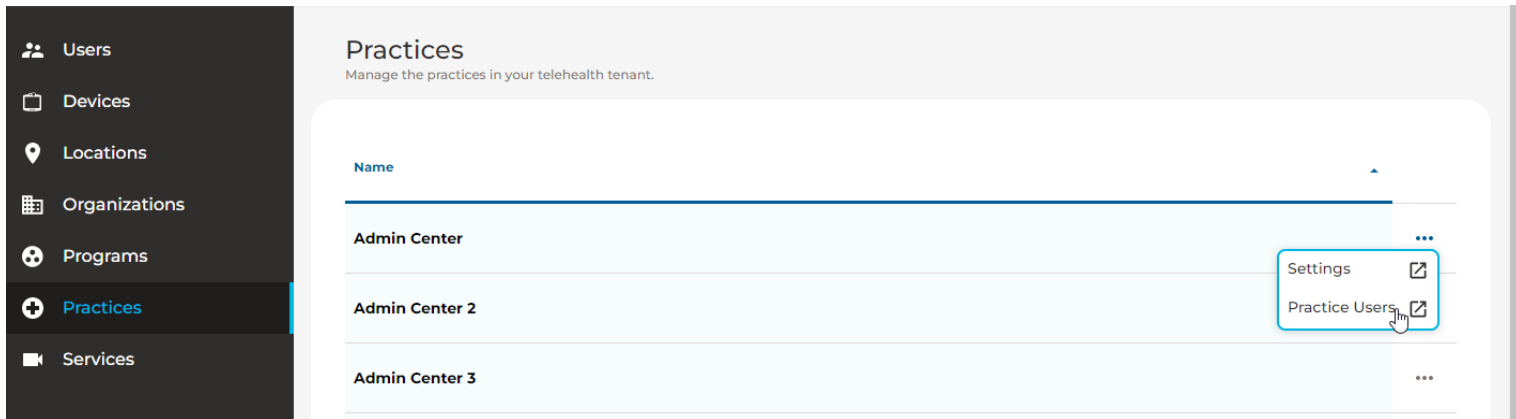
The following will be displayed.



Note: See MA-20165 Teladoc Health Practice Admin User Guide for more information about configuring practice settings.

## Configuring Practice Users

1. Click **Practices** in the left navigation panel.
2. Click the three horizontal dots for the practice and select **Practice Users**.



The following will be displayed.

<

Practice Settings

Practice Labels

Patient Profile

Practice Users

Default User Settings

Care Locations

Locations

Integrations

Departments / Programs

↩ Exit Settings

Practice Users

Create New User

	FULL NAME <span style="float: right;">▼</span>	EMAIL <span style="float: right;">▲</span>	ROLE <span style="float: right;">▲</span>	LAST ACTIVITY <span style="float: right;">▲</span>			
1.	[blurred]	[blurred]	Organization Admin	03/24/2021 10:33 AM	⚙	Disable	Reset Password
2.	[blurred]	[blurred]	Practitioner	09/16/2021 01:47 PM	⚙	Disable	Reset Password
3.	[blurred]	[blurred]	Organization Admin	09/13/2021 11:54 AM	⚙	Disable	Reset Password
4.	[blurred]	[blurred]	Practice Admin + Practitioner		⚙	Enable	Reset Password
5.	[blurred]	[blurred]	Practice Admin + Practitioner		⚙	Disable	Reset Password
6.	[blurred]	[blurred]	Practice Admin + Practitioner	09/23/2021 10:19 AM	⚙	Disable	Reset Password
7.	[blurred]	[blurred]	Organization Practitioner		⚙	Disable	Reset Password
8.	[blurred]	[blurred]	Practitioner		⚙	Disable	Reset Password
9.	[blurred]	[blurred]	Practitioner + Practice Admin	08/26/2022 01:22 PM	⚙	Enable	Reset Password

Note: See MA-20165 Teladoc Health Practice Admin User Guide for more information about configuring practice users.

## Services

Use the Services page to view and configure all the services, formerly waiting rooms, in a Tenant.

Note: The Services page is not displayed if you have a Classic account. Contact your Teladoc Health representative if you have questions.

Name	Practice	
AC 2 Dermatology	Admin Center 2	...
AC Behavioral Health	Admin Center	...
AC Family Med	Admin Center	...

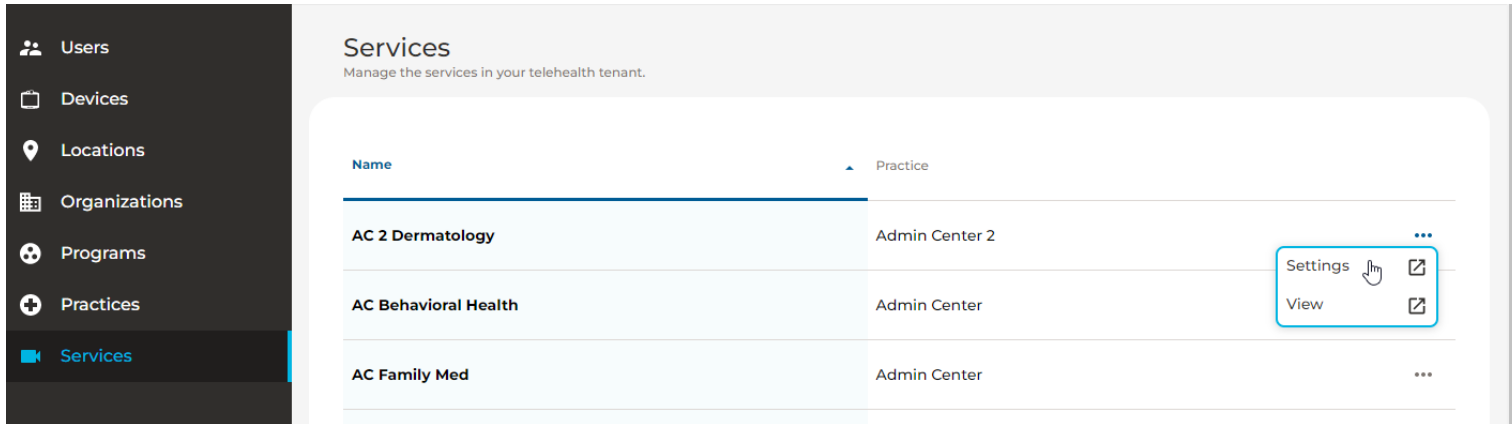
Click here to view and edit service settings and status.

Click the three horizontal dots in a row and then select Settings or View. This will open the service's configuration page or the service's information page for the service in a new browser window.

Note See MA-20165 Teladoc Health Practice Admin User Guide for more information about configuring services and see MA-20171 Teladoc Health Practitioner/Scheduler User Guide for more information about using services.

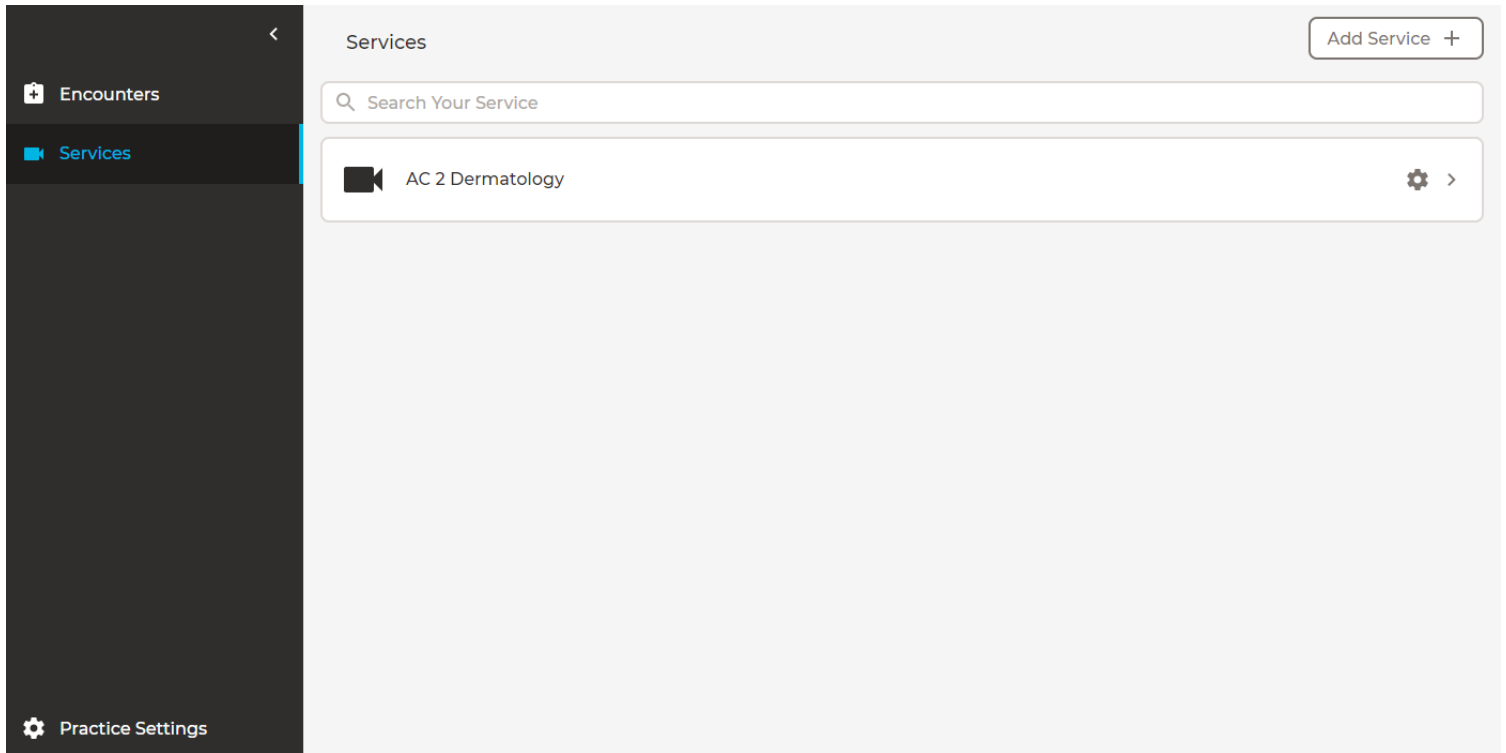
## Configuring Service Settings

1. Click **Services** in the left navigation panel.
2. Click the three horizontal dots for the practice and select **Settings**.



The following will be displayed.

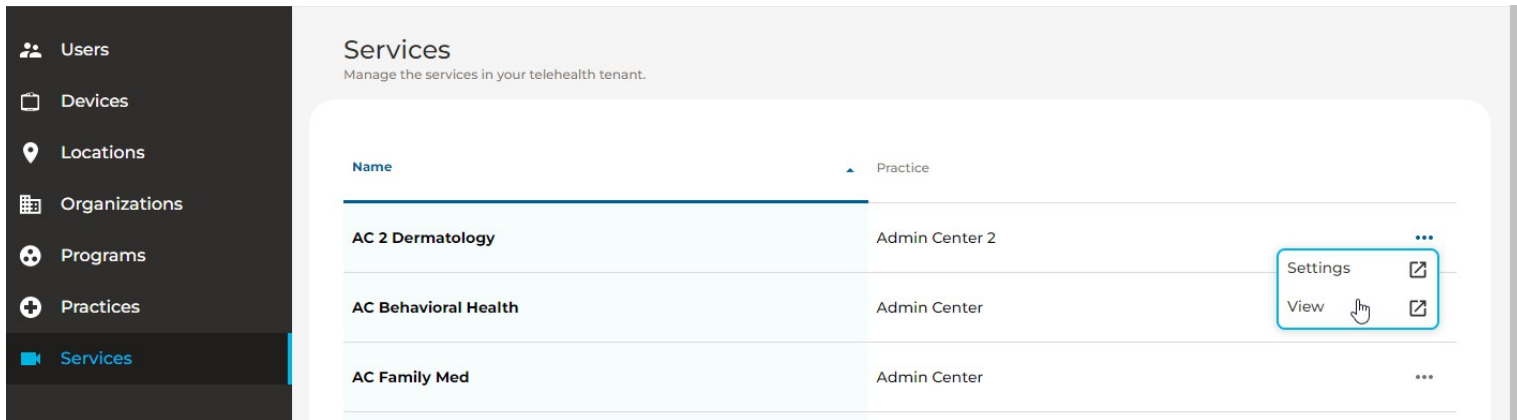




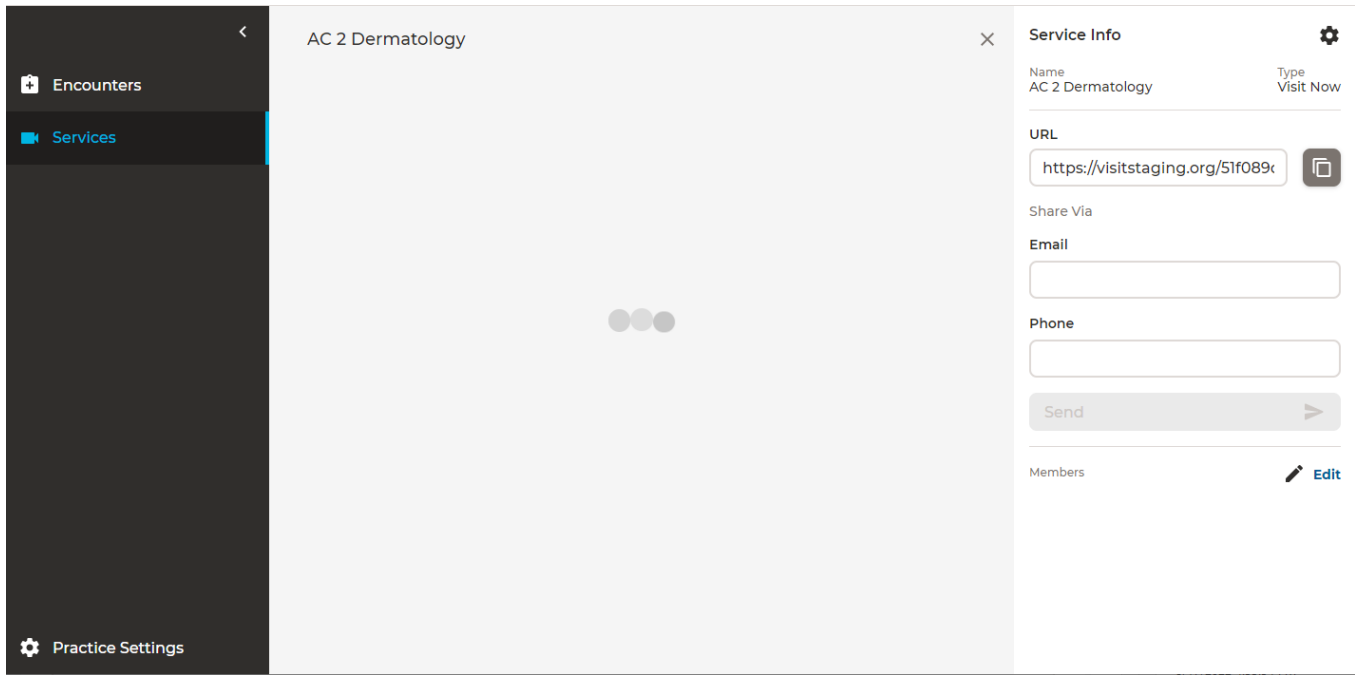
Note See MA-20165 Teladoc Health Practice Admin User Guide for more information about configuring service settings.

## Viewing Services

1. Click **Services** in the left navigation panel.
2. Click the three horizontal dots for the practice and select **View**.



The following will be displayed.



Note See MA-20171 Teladoc Health Practitioner/Scheduler User Guide for more information about using Solo services.

## HIPAA

As a business associate, Teladoc Health is subject to compliance of the law under 45 CFR §164.308 (Administrative Safeguards), under 45 CFR §164.310 (Physical Safeguards), and under 45 CFR §164.312 (Technical Safeguards) to maintain and transmit protected health information in electronic form in connection with transactions performed by the customer (covered entity).

The policy of this organization is to ensure, to the greatest extent possible, that Protected Health Information (PHI) is not intentionally or unintentionally used or disclosed in violation of the HIPAA Privacy Rule or any other federal or state regulations governing confidentiality and privacy of health information.

There are a number of safeguards implemented into the telehealth system to ensure that the system complies with the latest HIPAA regulations. One of the key requirements is Teladoc Health's ongoing implementation and updating of its HIPAA security policies and procedures to ensure for the availability, security, and privacy of telehealth connections and ePHI (electronic protected health information). Teladoc Health maintains a policy to ensure workforce HIPAA compliance and training. Teladoc Health additionally maintains HIPAA security policies and procedures, a data destruction policy, and security incident response procedures.

### Guidelines for Compliance

The telehealth system helps hospitals and medical professionals comply with HIPAA regulations. The tabs to the left describe some of the ways the telehealth system supports HIPAA compliance.

HIPAA requires all healthcare organizations to have policies and procedures, and the guidelines to the left. However, these may not cover all situations for a specific organization. For example, from time to time, automatic software upgrades may be downloaded which may contain new features. Teladoc Health will inform users of significant features added, their impact and how they may affect HIPAA policies, procedures, and safeguards.

## **Access to Provider Access**

The computer using the Provider Access should be placed in a location that is only accessible to individuals who have authorized access to Protected Health Information (PHI). It is recommended that Provider Access be password protected via a Windows or iOS user account.

Only authorized users should have passwords, and users should safeguard passwords according to hospital policies and procedures. Passwords should be treated as highly confidential information. If you believe your password may have been compromised, it should be changed as soon as possible. Change your password by clicking on the "Forgot Password" link on the login screen of the Teladoc Health Provider Access.

The Auto Logout feature is set to log out of the Teladoc Health Provider Access when the system is inactive for 30 minutes. Also, all users should be trained to log out of Windows, iOS or the Virtual Private Network

(VPN), when away from the system for any period of time. This is important for security reasons, so that any person attempting access to the Provider Access will be required to enter a password for secure access.

## Discussion and Display of PHI

From time to time a physician will likely engage in remote communications with patients and medical staff in which patient information (records, images and video) will be discussed or displayed. In general, the same care should be exercised as though the physician were physically present. For example:

- Use Head rotation to look around and see who else is nearby and might see or hear the sensitive information, and use appropriate discretion.
- Use the microphone mute button when conversing with someone alongside the Teladoc Health Provider Access to avoid the inadvertent conferencing of patient-related conversation.
- The Teladoc Health Provider Access screen should be positioned to point away from public areas, so as not to be visible to a passerby.

## Images and Video

By default, when saved, all captured images and video files are stored encrypted files; viewable only by the Provider Access user who captured them. All files are saved in the user's Teladoc Health Media Vault to provide added protection.

For convenience, these files may be saved in common formats, e.g., JPEG for still images. These files are no longer encrypted and therefore are viewable by any user who can access them. As such, there are a few recommended techniques for safeguarding PHI contained in these images and video:

- Ensure all personnel who have access to the Provider Access Software also have full permission to access stored images and videos under the hospital's policies and procedures.
- Make sure to store captured images and videos only on removable media (e.g., recordable CD-ROMs) which can be taken with each user or on secure network drives.
- Do not save any captured images and video clips. Use these images and video segments only while logged in for a virtual encounter.

## Disclosure of PHI

If the physician plans to transmit or copy stored images or video to other individuals or organizations, e.g., to a healthcare operator, the physician needs to abide by standard HIPAA codes governing who may receive PHI and under what conditions. The hospital's HIPAA compliance officer should be consulted for details.

# Contact Information

## 24/7 Live Technical Support

1-877-484-9119

## Email Support

[tac@teladochealth.com](mailto:tac@teladochealth.com)

## Teladoc Health User Manuals

<https://solosupport.teladochealth.com>

## Sales & Product Demos

1-805-562-8686

## Manufactured by

Teladoc Health  
7406 Hollister Avenue, Goleta, CA 93117  
Phone: +1.805.562.8686



[teladochealth.com](https://teladochealth.com) | [engage@teladochealth.com](mailto:engage@teladochealth.com)

**Teladoc Health** is the global virtual care leader, helping millions of people resolve their healthcare needs with confidence. Together with our clients and partners, we are continually modernizing the healthcare experience and making high-quality healthcare a reality for more people and organizations around the world.

© Teladoc Health, Inc. All rights reserved.

