



User Management Guide

V6 – June 2025

Contents

Overview	3
Domain Administrator and Security Manager(s)	3
Setting up Security Managers	3
Managing users	4
Accessing the Users screen	4
Finding a user	5
Understanding the user tabs	6
Using the General tab	7
Adding a new user	7
Updating a user's information	9
Deactivating a user	10
Reactivating users	11
Hiding the Support and Training Center link	12
Viewing history	13
Viewing password history	14
Using the Accounts tab	15
Using the Permissions tab	16
Using the Landing Page tab	17
Using the Roles tab	18
Creating a new role	18
Assigning a role to multiple users	19
Assigning a role to individual users	20
Using the Reset Password tab	21
Using the 2FA tab	22
Setting security	24
Setting password options	24
Working with IP addresses	25
Restricting login by IP address	25
Removing an IP address restriction	26
Working with Permission Sets	27
Overview	27
Creating a custom permission set	28
Edit an existing permission set	29
Enabling and using two-factor authentication	30
Enabling (requiring) two-factor authentication	30
Using two-factor authentication	33
Using the System Access Report	35
Revision log	36

Overview

Go to **ACCOUNT > Security**.

Waystar's Security Administration System allows your organization to define which areas of the Waystar system each user can access. To accomplish this, **one user** in your organization is assigned to be your organization's Domain Administrator while others can be assigned the role of Security Manager.

The safety and security of your information is Waystar's highest priority, that is why we follow strict security protocols to prevent any unauthorized access to your data. In the event you need to change your Domain Administrator, Waystar will reassign this function only after receiving a written request on your company's letterhead.

Domain Administrator and Security Manager(s)

The Domain Administrator and the Security Manager(s) can do the following:

- Add new users to the system
- Manage roles
- Set permissions, which indicates what each user is able to do within the system
- Reset passwords for users who have forgotten their password
- Inactivate users from the system
- Unlock users (after five consecutive failed logins, the system will automatically lock a user)
- Manage domain security settings/password rotation.

Anyone who uses the site must be set up as a user with their own username and password; this is for your security and ours.

Users will be deactivated if they do not log in to Waystar within a specified time. The default setting is one year but can be set to as little as one month. If the Domain Administrator is deactivated, a Security Manager can reactivate the account.

Note: Be sure to let your users know who the Domain Administrator and Security Manager(s) are and that users can contact them to have a password reset. Also, if the user has confirmed their email address via the Waystar portal, they can reset their own password when logging into the portal and clicking the **Forgot your username or password?** link on the WELCOME login screen.

Setting up Security Managers

IMPORTANT: Waystar strongly recommends that you designate **at least one Security Manager** with permissions to add users and reset passwords in the event that the Domain Administrator is not available when a user needs to reset their password.

To set users as Security Managers, see the [Setting a user's role](#) section.

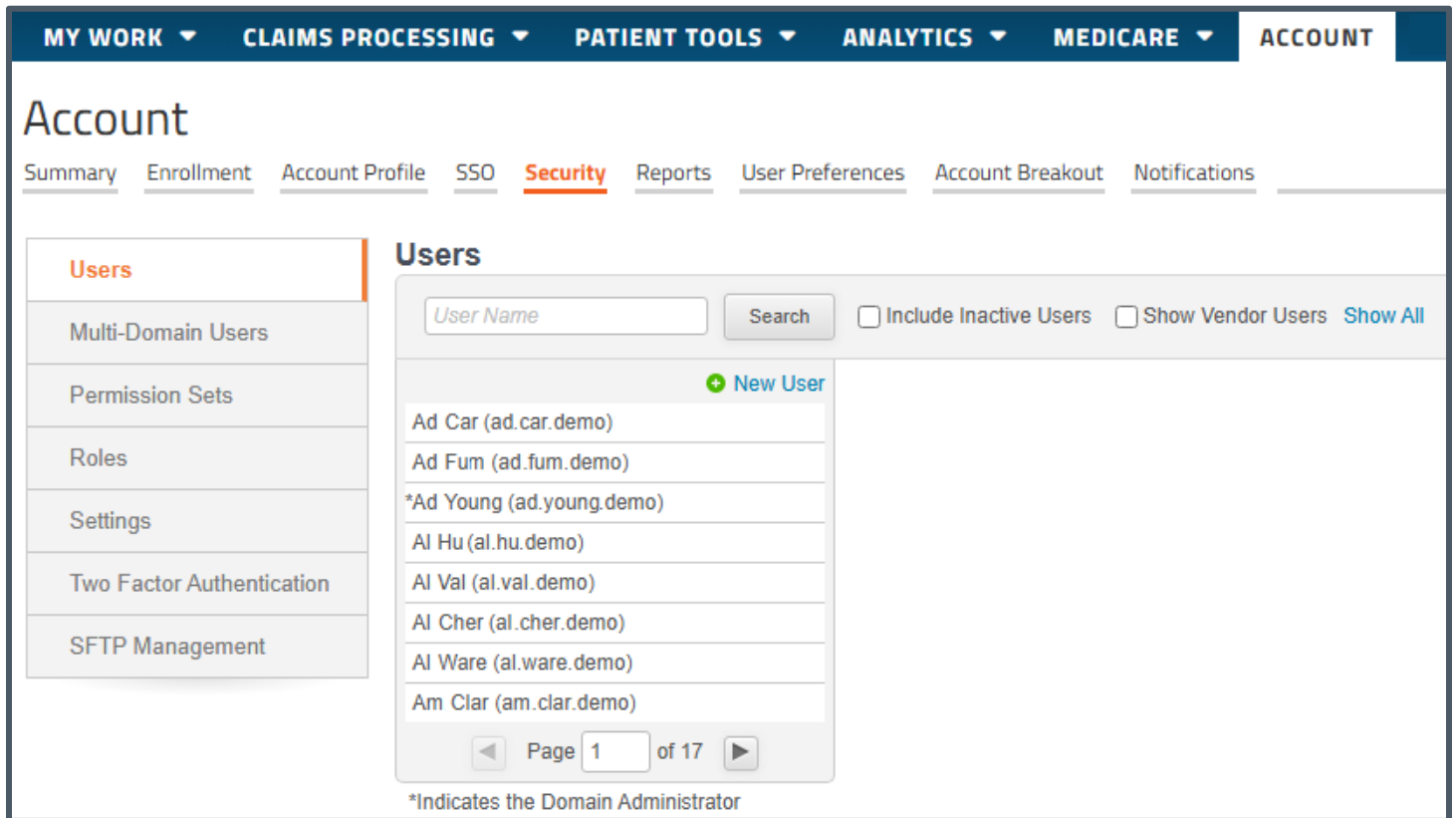
Managing users

This section explains for the Domain Administrator and Security Managers how to manage security settings in the Waystar portal.

Accessing the Users screen

Note: All Domain Administrators and Security Managers have access to the ACCOUNT > **Security** tab. However, not all end-users have access to this tab, which is based on your organization's settings.

Go to **ACCOUNT > Security > Users**. This is where you will manage all your users.



From the Users screen, you can:

- [Add new users](#)
- [Set general information](#)
- [Set accounts](#)
- [Set permissions](#)
- [Set roles](#)
- [Reset passwords](#)
- [Update](#) or [deactivate](#) any users.

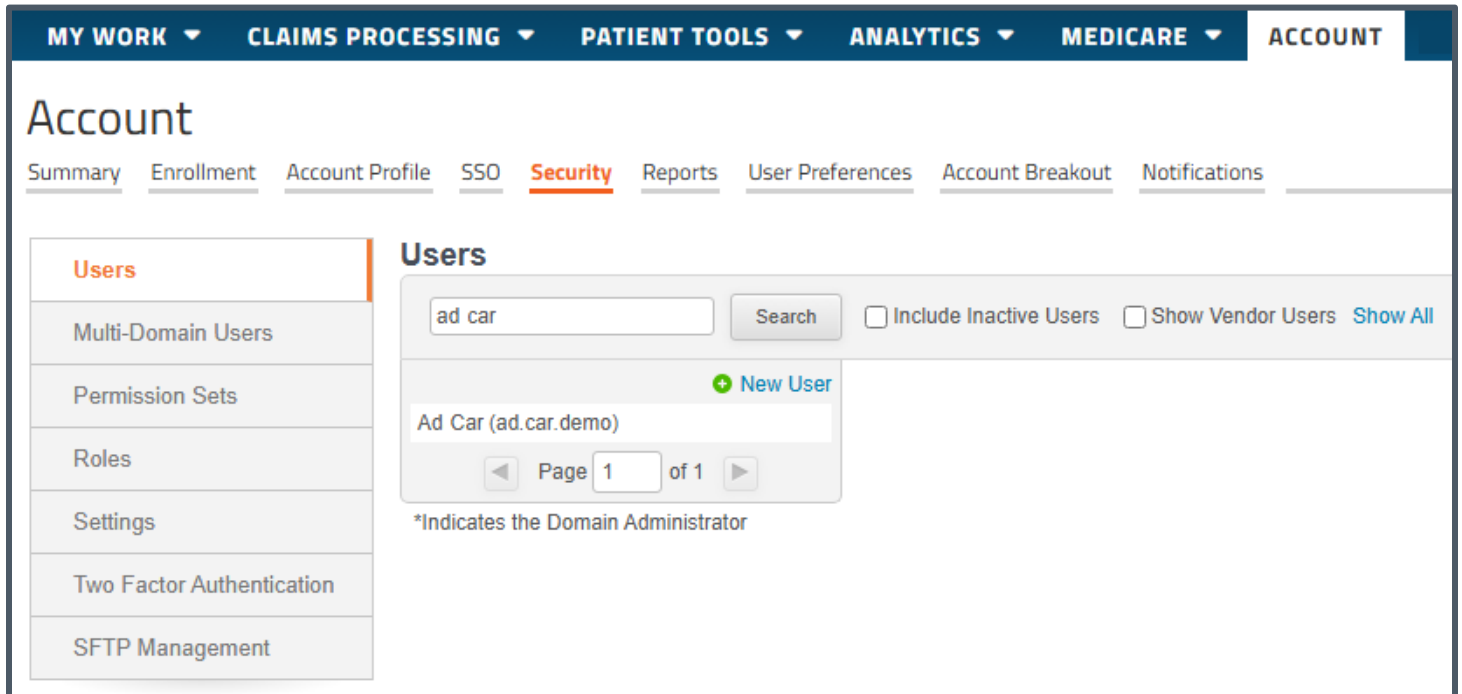
Finding a user

This section explains how to find a user within your list.

To find a user, go to the **ACCOUNT > Security > Users** screen and perform any of the following:

- **Additional users:** You can include inactive and vendor users in your list by selecting the **Include Inactive Users** and/or **Show Vendor Users** checkboxes at the top of the list. When selecting, those users will also appear in search results.
- **Scroll:** You can scroll the list using the page forward and backward arrow buttons at the bottom of the list.
- **Page:** You can go directly to a page by putting the page number into the **Page** field, and then clicking the forward arrow button.
- **Search:** In the Search field at the top of the list, type their name in the Search field, and then click the **Search** button. You can search by their entire name, their first or last name, or by using a partial match.
- **Show All:** Click the **Show All** link to remove any search criteria and redisplay the entire list of users.

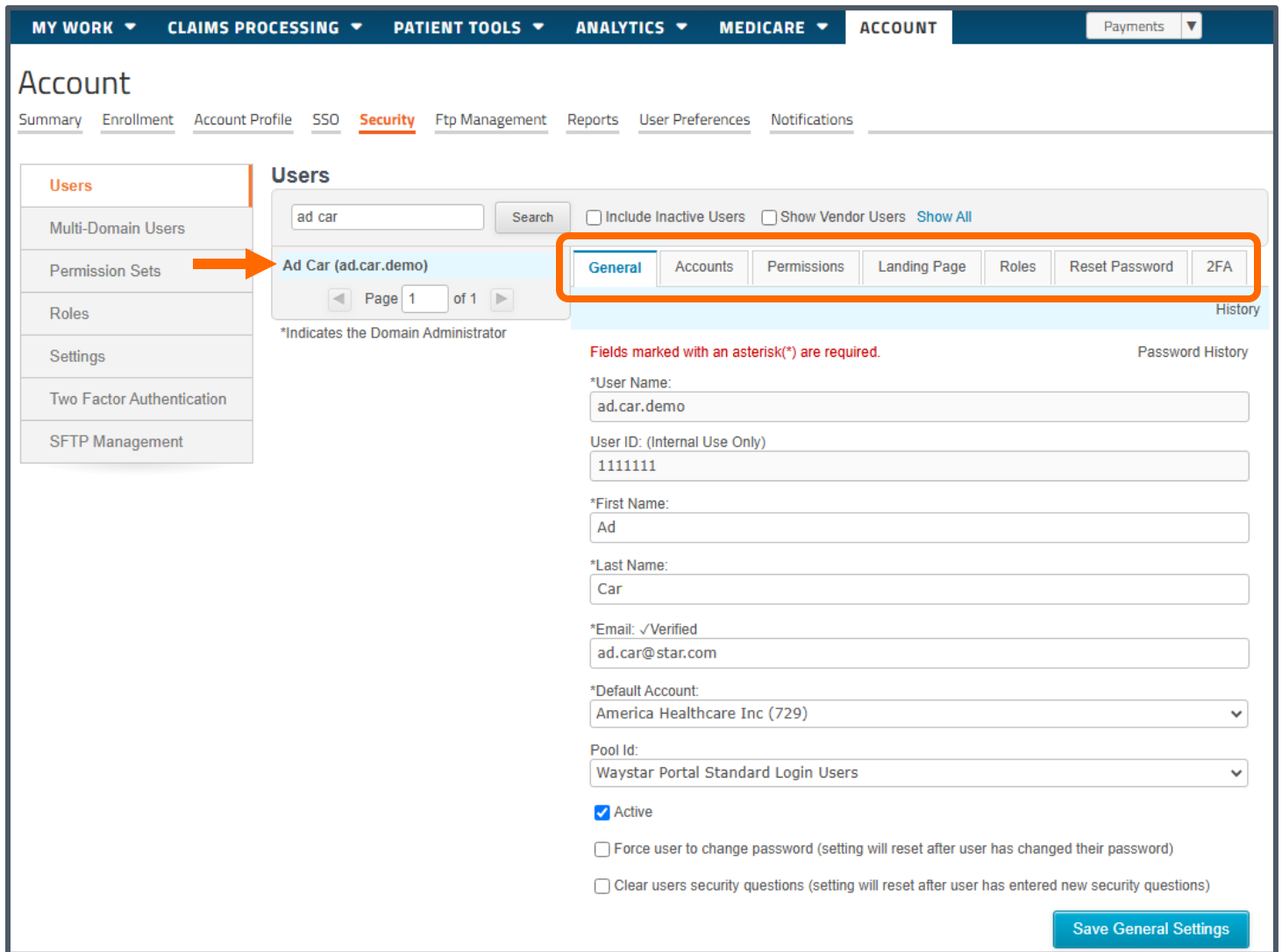
The following example shows a search by a user's full name.



The screenshot displays the Waystar Account interface. The top navigation bar includes links for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT section is active, showing a sub-menu with Summary, Enrollment, Account Profile, SSO, Security (highlighted), Reports, User Preferences, Account Breakout, and Notifications. The main content area is titled 'Account' and features a sidebar with links to Users, Multi-Domain Users, Permission Sets, Roles, Settings, Two Factor Authentication, and SFTP Management. The 'Users' section is expanded, showing a search bar with the text 'ad car' and a 'Search' button. Below the search bar are checkboxes for 'Include Inactive Users' and 'Show Vendor Users', and a 'Show All' link. A '+ New User' button is also visible. The search results show a single user, 'Ad Car (ad.car.demo)', with a pagination bar indicating 'Page 1 of 1'. A note at the bottom states '*Indicates the Domain Administrator'.

Understanding the user tabs

This section provides an overview of the user tabs that will appear after you [find a user](#) and click their name.



Account

Summary Enrollment Account Profile SSO **Security** Ftp Management Reports User Preferences Notifications

Users

ad car Search ☐ Include Inactive Users ☐ Show Vendor Users [Show All](#)

Ad Car (ad.car.demo)

Page 1 of 1

*Indicates the Domain Administrator

General Accounts Permissions Landing Page Roles Reset Password 2FA

Fields marked with an asterisk(*) are required. Password History

*User Name: ad.car.demo

User ID: (Internal Use Only) 1111111

*First Name: Ad

*Last Name: Car

*Email: ✓Verified ad.car@star.com

*Default Account: America Healthcare Inc (729)

Pool Id: Waystar Portal Standard Login Users

☒ Active

☐ Force user to change password (setting will reset after user has changed their password)

☐ Clear users security questions (setting will reset after user has entered new security questions)

[Save General Settings](#)

Click the following links to go to the corresponding section in this guide.

- [General](#): Use to review and update a user's general information, such as their name, default account, and whether they are active.
- [Accounts](#): Use to grant permissions to a specific account. When a user has a permission, that permission is applied to all accounts to which the user has access.
- [Permissions](#): Use to set permissions for a user for accounts they were granted access to.
- [Landing Page](#): Use to set the default Waystar portal landing page for the user.
- [Roles](#): Use to set the roles in which a user can function.
- [Reset Password](#): Use to change the password of a user.
- [2FA](#): Use to set a one-time code for users who lose access to their account.

Using the General tab

The **ACCOUNT > Security > Users** tab is where you perform the most basic user management security tasks, such as adding, updating, activating, and inactivating users.

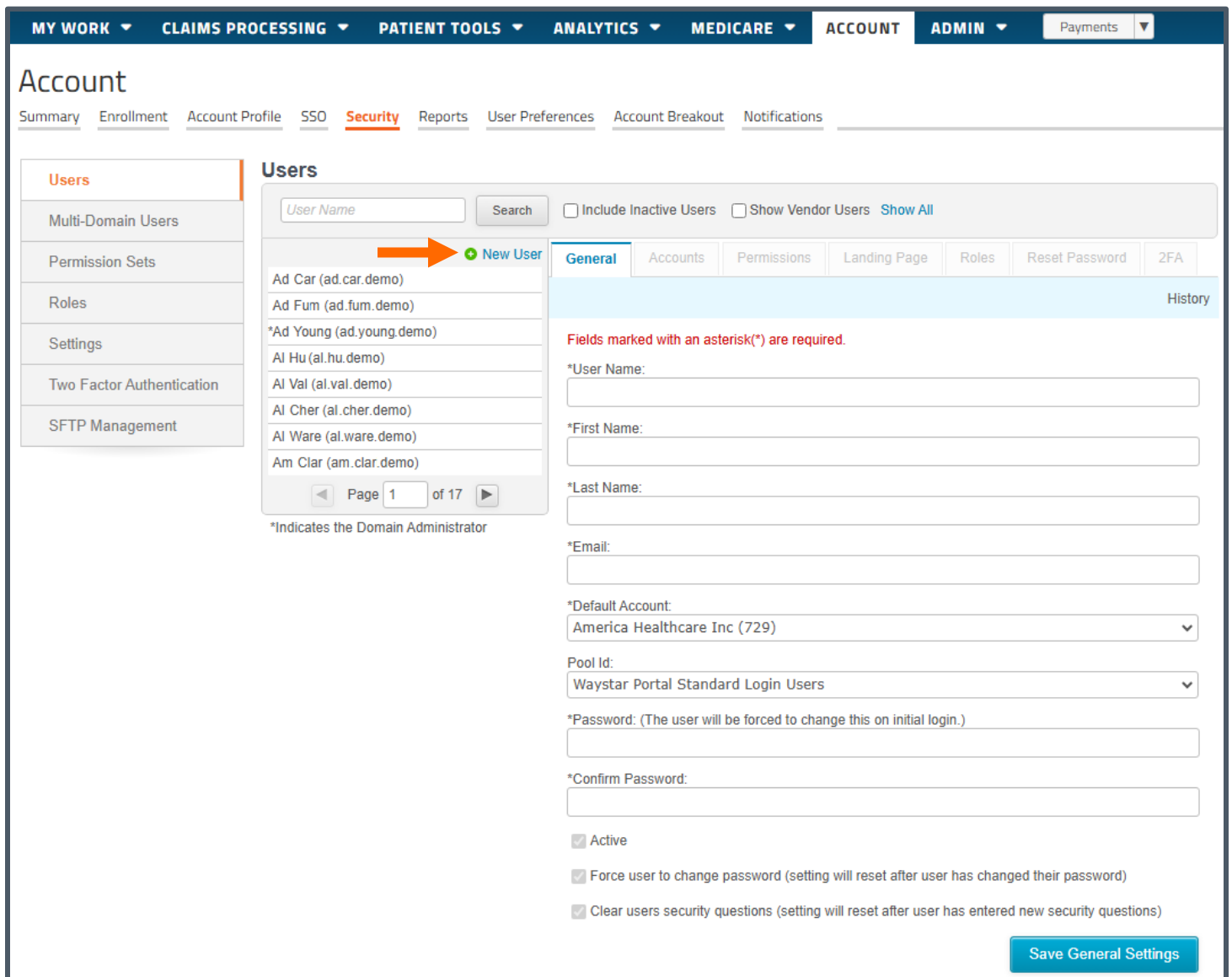
Adding a new user

This section explains how Domain Administrators and Security Managers can add a new user so that you can give them access to your organization's Waystar portal.

To add a new user:

1. Go to **ACCOUNT > Security > Users**.
2. Click the **New User** link.

The General tab will display mostly blank fields.



The screenshot shows the Waystar Account > Security > Users page. The 'New User' link is highlighted with an orange arrow. The 'General' tab is selected, showing fields for User Name, First Name, Last Name, Email, Default Account, Pool Id, Password, and Confirm Password. A 'Save General Settings' button is at the bottom right.

Account

Summary Enrollment Account Profile SSO **Security** Reports User Preferences Account Breakout Notifications

Users

Multi-Domain Users

Permission Sets

Roles

Settings

Two Factor Authentication

SFTP Management

Users

User Name Search ☐ Include Inactive Users ☐ Show Vendor Users [Show All](#)

[New User](#)

Ad Car (ad.car.demo)

Ad Fum (ad.fum.demo)

*Ad Young (ad.young.demo)

Al Hu (al.hu.demo)

Al Val (al.val.demo)

Al Cher (al.cher.demo)

Al Ware (al.ware.demo)

Am Clar (am.clar.demo)

Page 1 of 17

*Indicates the Domain Administrator

General Accounts Permissions Landing Page Roles Reset Password 2FA History

Fields marked with an asterisk(*) are required.

*User Name:

*First Name:

*Last Name:

*Email:

*Default Account:

America Healthcare Inc (729)

Pool Id:

Waystar Portal Standard Login Users

*Password: (The user will be forced to change this on initial login.)

*Confirm Password:

☒ Active

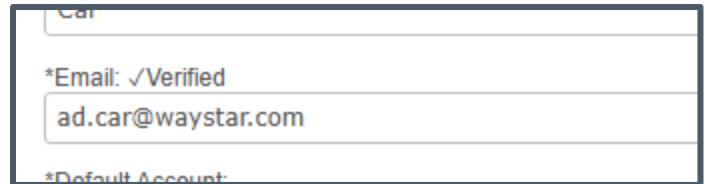
☒ Force user to change password (setting will reset after user has changed their password)

☒ Clear users security questions (setting will reset after user has entered new security questions)

[Save General Settings](#)

3. Enter the following information:

- **User Name:** Provide a username. We recommend the user's first and last names with a period (dot) in the middle, such as jill.smith. The maximum allowable length is 100 characters and can include numeric and special characters, except for < > * % & : ? \
- **First Name:** Provide the user's first name.
- **Last Name:** Provide the user's last name.
- **Email:** Provide the user's company email address. The email address must be verified by the user when they first log into the Waystar portal. When verified, the Verified icon will appear next to the field.
- **Default Account:** If your organization has multiple accounts, select from the dropdown the account you want the user to have as their default. If your organization has a single account, it will automatically populate in the field.
- **Pool Id:** Establishes how you expect the user to authenticate their login to the Waystar portal.
 - **Waystar Portal Standard Login Users:** A user who uses the standard Waystar login screen.
 - **Real-time API Users:** A user who uses a third-party tool, such as Okta, for login authentication.
- **Password/Confirm Password:** This is a temporary password that is valid for 24 hours; the system will force the user to change this password.
 - Contains at least 15 characters
 - Contains at least one number
 - Contains at least one uppercase AND one lowercase character
 - Contains at least one special character
 - Cannot contain any of the following special characters < > * % & : \ ?
 - Cannot contain the user's first name, last name, or Waystar username
 - Cannot have consecutively repeating characters
 - Cannot repeat previous 24 passwords
 - Cannot be a commonly used password.



The screenshot shows a portion of a web form. It includes a text input field for an email address, which contains 'ad.car@waystar.com'. Above the email field, there is a status indicator that reads '*Email: ✓Verified'. Below the email field, there is a dropdown menu labeled '*Default Account:'.

For additional information, see the [Setting password options](#) section.

- **Active:** Selected by default, when you add the user, they will automatically be active.
- **Force user to change password:** Selected by default, the system will force the user to change their password when they first log in. After they change their password, this checkbox will be clear (not selected).
- **Clear users security questions:** Selected by default, the system will ask the user for security questions when they first log in. After they answer the questions, this checkbox will be clear (not selected).

4. Click the **Save General Settings** button.

As shown in the following section, the system will automatically generate and display the user's user ID.

Updating a user's information

This section explains how Domain Administrators and Security Managers can update a user's general information.

To change a user's information:

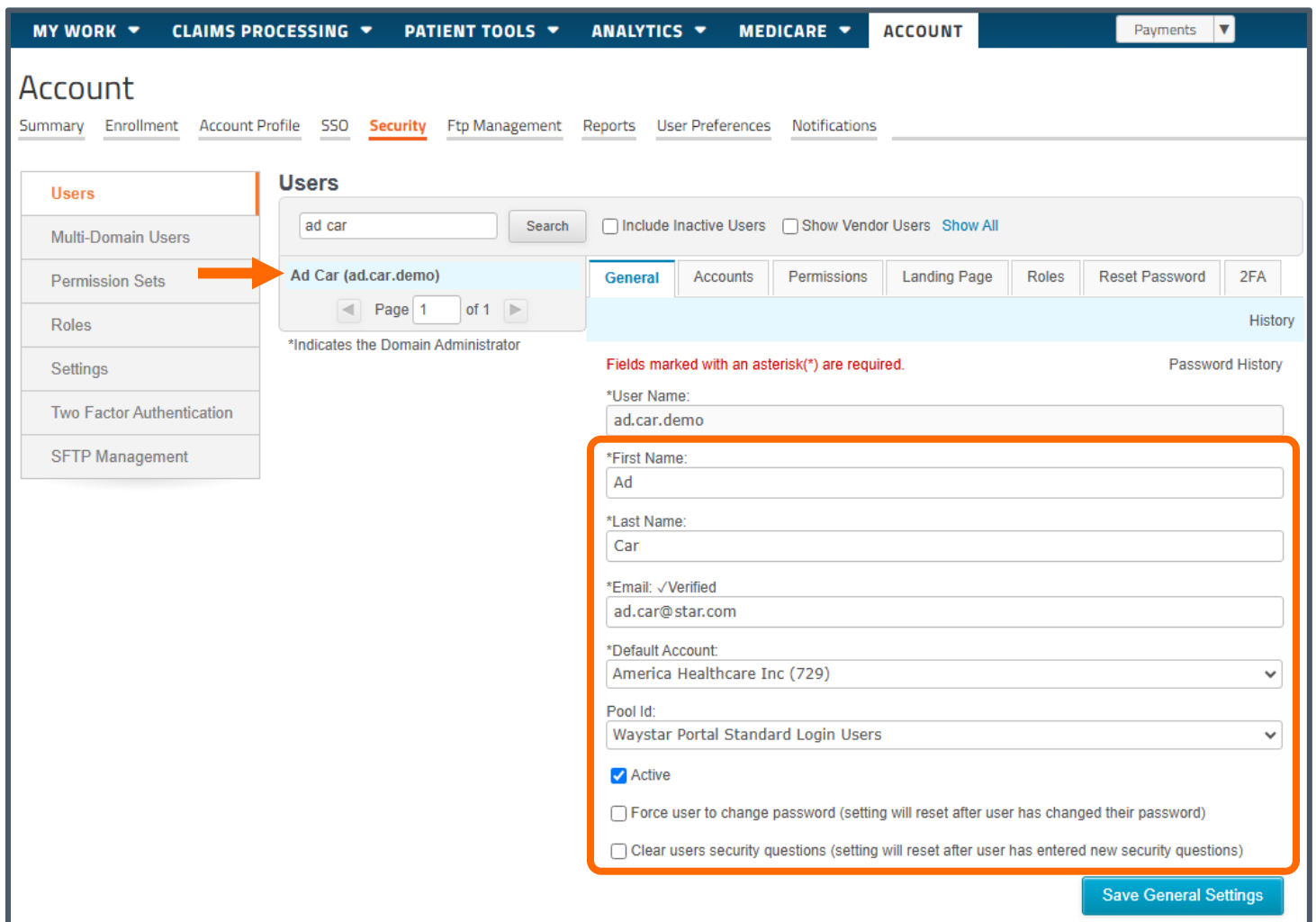
1. Go to **ACCOUNT > Security > Users**.
2. Select a user.

The General tab will display the user's information.

3. From the General tab, change field information as appropriate. For field descriptions, see the [Adding a new user](#) section.

Note: You cannot change the User Name field.

4. When finished updating fields, click the **Save General Settings** button.



The screenshot shows the Waystar Account interface. The top navigation bar includes 'MY WORK', 'CLAIMS PROCESSING', 'PATIENT TOOLS', 'ANALYTICS', 'MEDICARE', and 'ACCOUNT'. The 'ACCOUNT' tab is selected, and a 'Payments' dropdown is visible. Below the navigation bar, the 'Account' section has tabs for 'Summary', 'Enrollment', 'Account Profile', 'SSO', 'Security', 'Ftp Management', 'Reports', 'User Preferences', and 'Notifications'. The 'Security' tab is selected, and the 'Users' sub-tab is active. On the left, a sidebar menu lists 'Users', 'Multi-Domain Users', 'Permission Sets', 'Roles', 'Settings', 'Two Factor Authentication', and 'SFTP Management'. An orange arrow points to the 'Users' section. The main content area shows a search bar with 'ad car' and a 'Search' button. Below the search bar, a list of users is shown, with 'Ad Car (ad.car.demo)' selected. The 'General' tab for this user is active, displaying fields for 'User Name', 'First Name', 'Last Name', 'Email', 'Default Account', 'Pool Id', and 'Active' status. The 'Active' checkbox is checked. At the bottom right, there is a 'Save General Settings' button.

Users

ad car Search ☐ Include Inactive Users ☐ Show Vendor Users [Show All](#)

Ad Car (ad.car.demo)

Page 1 of 1

*Indicates the Domain Administrator

General Accounts Permissions Landing Page Roles Reset Password 2FA

History

Fields marked with an asterisk(*) are required.

*User Name: ad.car.demo

*First Name: Ad

*Last Name: Car

*Email: ✓Verified ad.car@star.com

*Default Account: America Healthcare Inc (729)

Pool Id: Waystar Portal Standard Login Users

☒ Active

☐ Force user to change password (setting will reset after user has changed their password)

☐ Clear users security questions (setting will reset after user has entered new security questions)

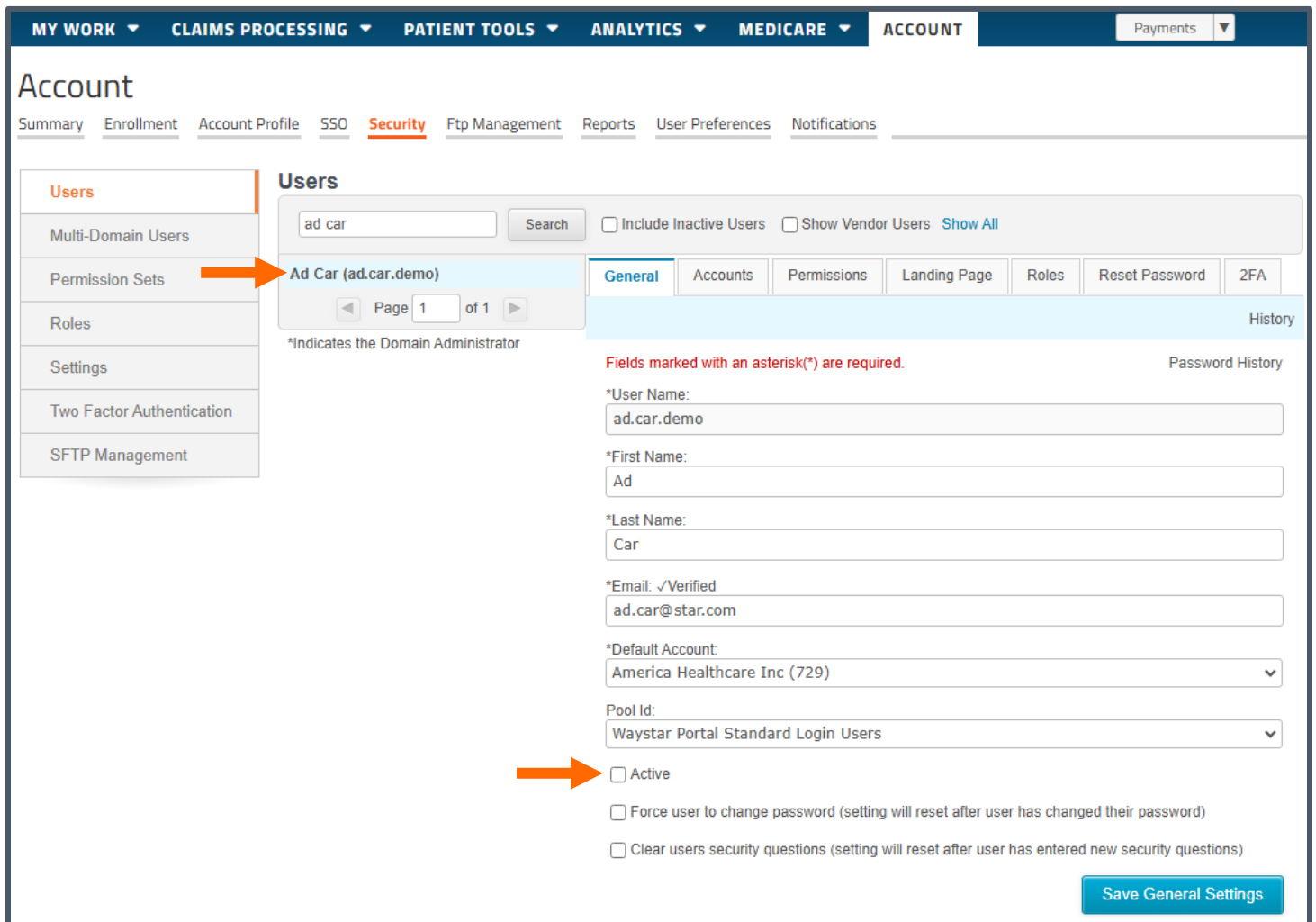
Save General Settings

Deactivating a user

This section explains how Domain Administrators and Security Managers can deactivate a user, which will prevent that user from logging into your organization's Waystar portal.

To deactivate a user:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. From the General tab, clear (unselect) the **Active** checkbox.
4. Click the **Save General Settings** button.
5. To reactivate the user account, select the **Active** button and click the **Save General Settings** button.



The screenshot shows the Waystar Account Security Users page. The top navigation bar includes tabs for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is selected, and a dropdown menu shows 'Payments'. Below the navigation bar, the 'Account' section is active, with sub-tabs for Summary, Enrollment, Account Profile, SSO, Security, Ftp Management, Reports, User Preferences, and Notifications. The 'Security' sub-tab is selected, and the 'Users' section is highlighted in the left sidebar. An orange arrow points to the 'Users' section in the sidebar. The 'Users' section displays a list of users, with 'Ad Car (ad.car.demo)' selected. An orange arrow points to this user. Below the user list, the 'General' tab is selected, and the user's details are displayed. The details include fields for User Name, First Name, Last Name, Email, Default Account, and Pool Id. The 'Active' checkbox is unchecked, and an orange arrow points to it. Below the 'Active' checkbox are two other checkboxes: 'Force user to change password' and 'Clear users security questions'. The 'Save General Settings' button is located at the bottom right of the form.

Users

ad car Search ☐ Include Inactive Users ☐ Show Vendor Users [Show All](#)

Ad Car (ad.car.demo) ☐ Page 1 of 1

*Indicates the Domain Administrator

General Accounts Permissions Landing Page Roles Reset Password 2FA

History

Fields marked with an asterisk(*) are required.

*User Name: ad.car.demo

*First Name: Ad

*Last Name: Car

*Email: ✓Verified ad.car@star.com

*Default Account: America Healthcare Inc (729)

Pool Id: Waystar Portal Standard Login Users

☐ Active

☐ Force user to change password (setting will reset after user has changed their password)

☐ Clear users security questions (setting will reset after user has entered new security questions)

Save General Settings

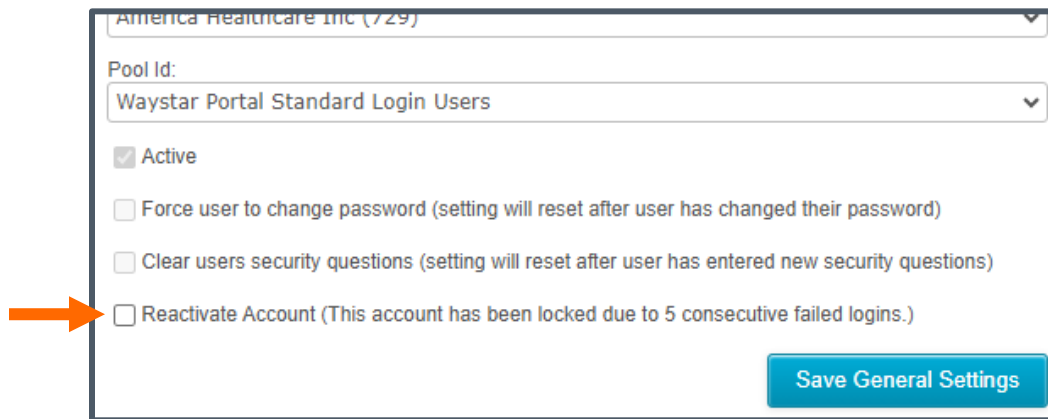
Reactivating users

This section explains how Domain Administrators and Security Managers can reactivate (unlock) a user after the user attempts **five** unsuccessful login attempts.

The Waystar system will display a notification message on the Waystar login screen when the user has failed five login attempts and their account is locked.

To reactivate (unlock) a user:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. From the General tab, select the **Reactivate Account (This account has been locked due to 5 consecutive failed logins.)** checkbox.
4. Click the **Save General Settings** button.



A screenshot of a web form for managing a user. At the top, there is a dropdown menu showing 'America Healthcare Inc (729)'. Below it is a 'Pool Id:' dropdown menu showing 'Waystar Portal Standard Login Users'. There are four checkboxes: 'Active' (checked), 'Force user to change password (setting will reset after user has changed their password)', 'Clear users security questions (setting will reset after user has entered new security questions)', and 'Reactivate Account (This account has been locked due to 5 consecutive failed logins.)'. An orange arrow points to the 'Reactivate Account' checkbox. At the bottom right is a blue button labeled 'Save General Settings'.

The Reactivate Account checkbox will disappear, and the **Active** checkbox will be active again.

5. Notify the user that you have unlocked their account.

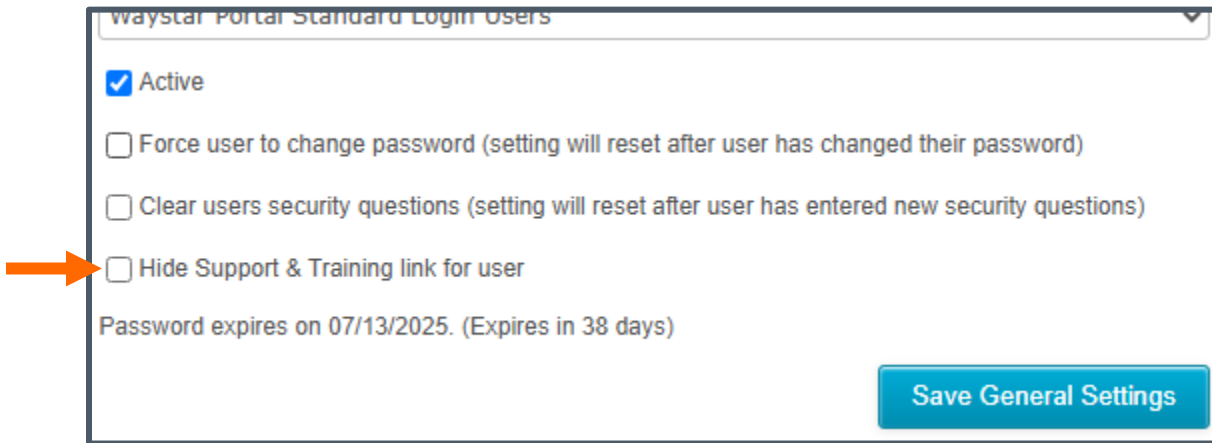
Hiding the Support and Training Center link

This option is primarily for Waystar Partners who need to hide the Support and Training Center (STC) from their users.

IMPORTANT: For our client organizations, we strongly recommend that you DO NOT hide the STC from your users so that they have access to valuable help articles and the ability to create Support cases.

To hide the STC link:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. From the General tab, select the **Hide Support & Training link for user** checkbox.
4. Click the **Save General Settings** button.



waystar Portal Standard Login Users

☒ Active

☐ Force user to change password (setting will reset after user has changed their password)

☐ Clear users security questions (setting will reset after user has entered new security questions)

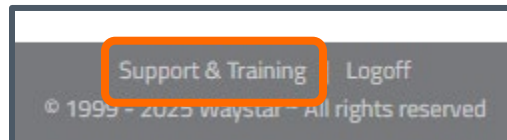
☐ Hide Support & Training link for user

Password expires on 07/13/2025. (Expires in 38 days)

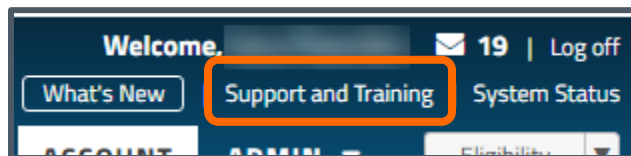
Save General Settings

The selected user will no longer see the STC link in the Waystar portal, such as in the following locations:

- At the bottom of a portal screen:



- At the top of a portal screen:

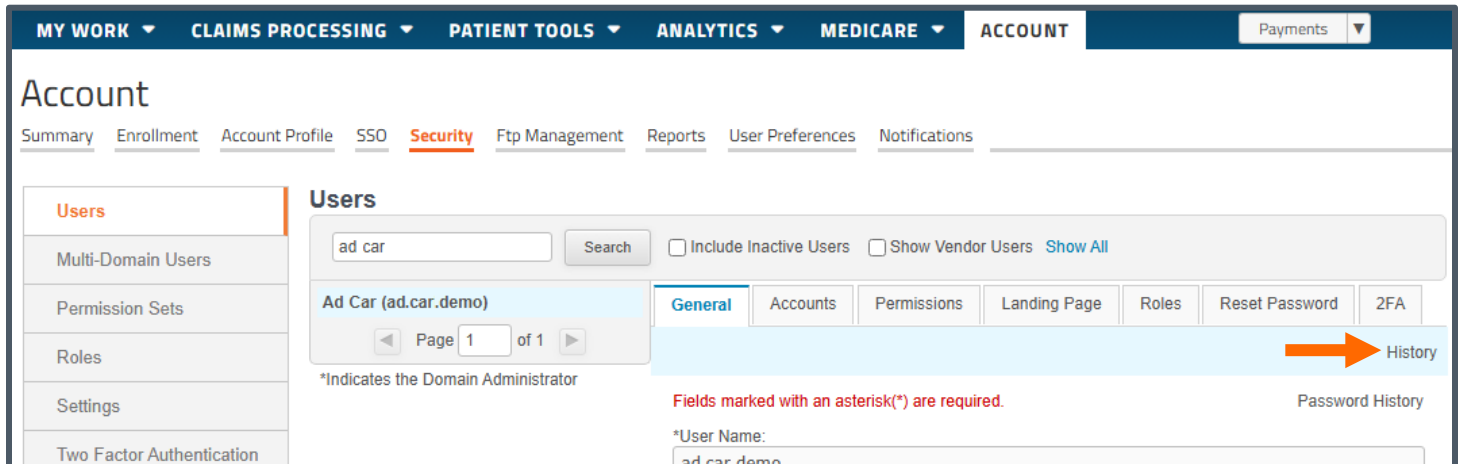


Viewing history

This section explains how to view the history of actions taken on the user via the General tab.

To view history:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. Click the **History** link on the right side of the blue bar at the top of the General tab.



The screenshot shows the 'Account' section with the 'Security' tab selected. Under 'Users', the user 'ad car' is selected. The 'General' tab is active. An orange arrow points to the 'History' link on the right side of the blue bar at the top of the General tab.

The User History screen will open with a list of any actions taken on this user account.

User History					X
Date	Time	User	Action	Changes	
6/17/2022	11:06 AM	ste.kra	UPDATED	ClearSecurityQuestions: False to True	
6/17/2022	11:05 AM	ste.kra	CREATED	Initial record created	

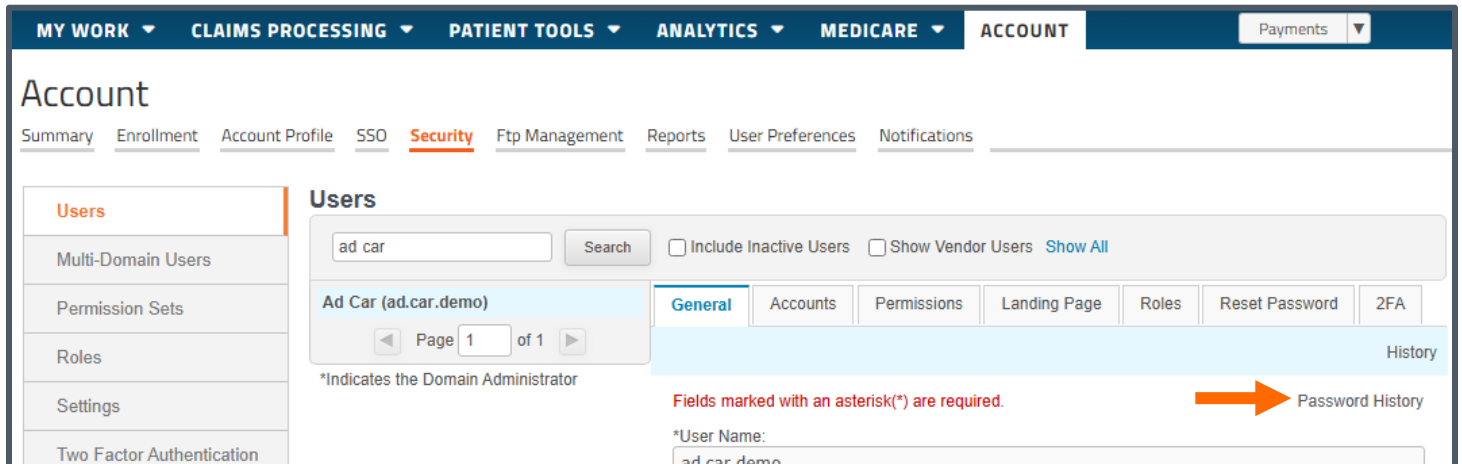
- **Date:** The date the action was made.
- **Time:** The time of day the action was made.
- **User:** The user (DA or SM) who action the change.
- **Action:** The action status.
- **Changes:** A description of the action.

Viewing password history

This section explains how to view the history of actions taken on the user via the General tab.

To view history:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. Click the **Password History** link near the top right of the General tab.



The Password History screen will open with a list of any actions taken on the password.

Password History		
Changed By	Password Expires	Date Changed
Ad Car	9/15/2022	6/17/2022 11:12 AM
Ste Kra	6/18/2022	6/17/2022 11:05 AM

- **Change By:** The user (DA/SM or the user themselves) who changed the password.
- **Password Expires:** The date the user's password will expire.
- **Date Changed:** The date the password was changed.

Using the Accounts tab

This section explains how Domain Administrators and Security Managers can grant user access to specific accounts within a domain.

To use the Accounts tab:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. To the right of the selected user, click the **Accounts** tab. All the child accounts for the domain are listed in alphabetic order after the Parent account.
4. *Optional.* To view hidden accounts, click the **Include Hidden Accounts** checkbox. To hide/unhide accounts, contact your Waystar Representative.
5. Complete one of the following:
 - Click individual checkboxes for each account to which the user will have access.
 - Click the **Check All** checkbox to select all accounts.
6. *Optional.* To view a list of users with access to a particular account, click the **Report** link to the right of an account name.

The screenshot shows the Waystar 'Users' management interface. On the left is a sidebar with navigation links: Users, Multi-Domain Users, Permission Sets, Roles, Settings, Two Factor Authentication, and SFTP Management. The main area is titled 'Users' and contains a search bar, checkboxes for 'Include Inactive Users' and 'Show Vendor Users', and a 'Show All' link. Below this is a list of users. The user 'Ad Car (ad.car.demo)' is selected, and an orange arrow points to the 'Accounts' tab in the top right of the user's profile. The 'Accounts' tab displays a list of child accounts with checkboxes for selection and a 'Report' link for each. An orange arrow points to the 'Include Hidden Accounts' checkbox. Another orange arrow points to the 'Report' link for 'America Healthcare Hospital (4520)'. The list of accounts includes:

Account Name	Selected	Report
America Healthcare Inc (729)	<input checked="" type="checkbox"/>	Report
America Healthcare DME (81772)	<input type="checkbox"/>	Report
America Healthcare FQHC (226656)	<input type="checkbox"/>	Report
America Healthcare Home Health (81770)	<input type="checkbox"/>	Report
America Healthcare Hospital (4520)	<input checked="" type="checkbox"/>	Report
America Healthcare Physical Therapy (4518)	<input type="checkbox"/>	Report
America Healthcare Primary Care (188)	<input type="checkbox"/>	Report

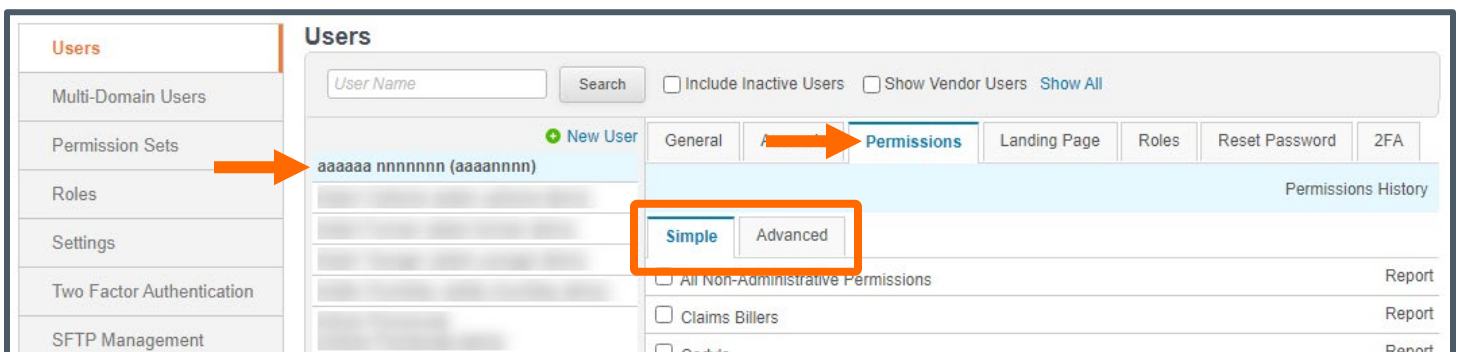
Using the Permissions tab

This section explains how Domain Administrators and Security Managers can assign or remove user permissions to solutions within the account(s) the user was granted access to.

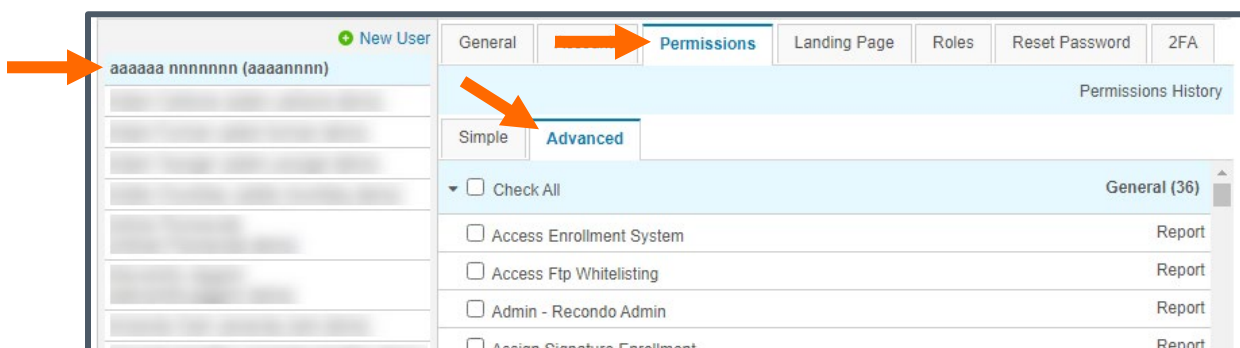
To use the Permissions tab:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. To the right of the selected user, click the **Permissions** tab.
4. To assign or remove permission sets, click the **Simple** subtab and select or clear the permission set checkbox(es). For more information, see the [Working with Permission Sets](#) section.

When you select a permission set from the Simple tab, all checkboxes for the individual permissions included in the set are automatically checked (selected), grayed out, and cannot be changed on the Advanced tab.



5. To assign or remove individual permissions, click the **Advanced** subtab and perform any of the following:
 - To find the specific permission, either scroll the list or press **[ctrl] [f]** and use your browser's search function to locate a permission.
 - To assign or remove permissions, click individual checkbox(es).
 - To assign or remove all permissions for a solution, select or clear the **Check All** checkbox that appears in the blue heading bar for each solution.



6. *Optional.* To view a list of users granted permissions to a particular permission set or permission, go to the **Simple** or **Advanced** subtab, and click the **Report** link to the right of a permission.

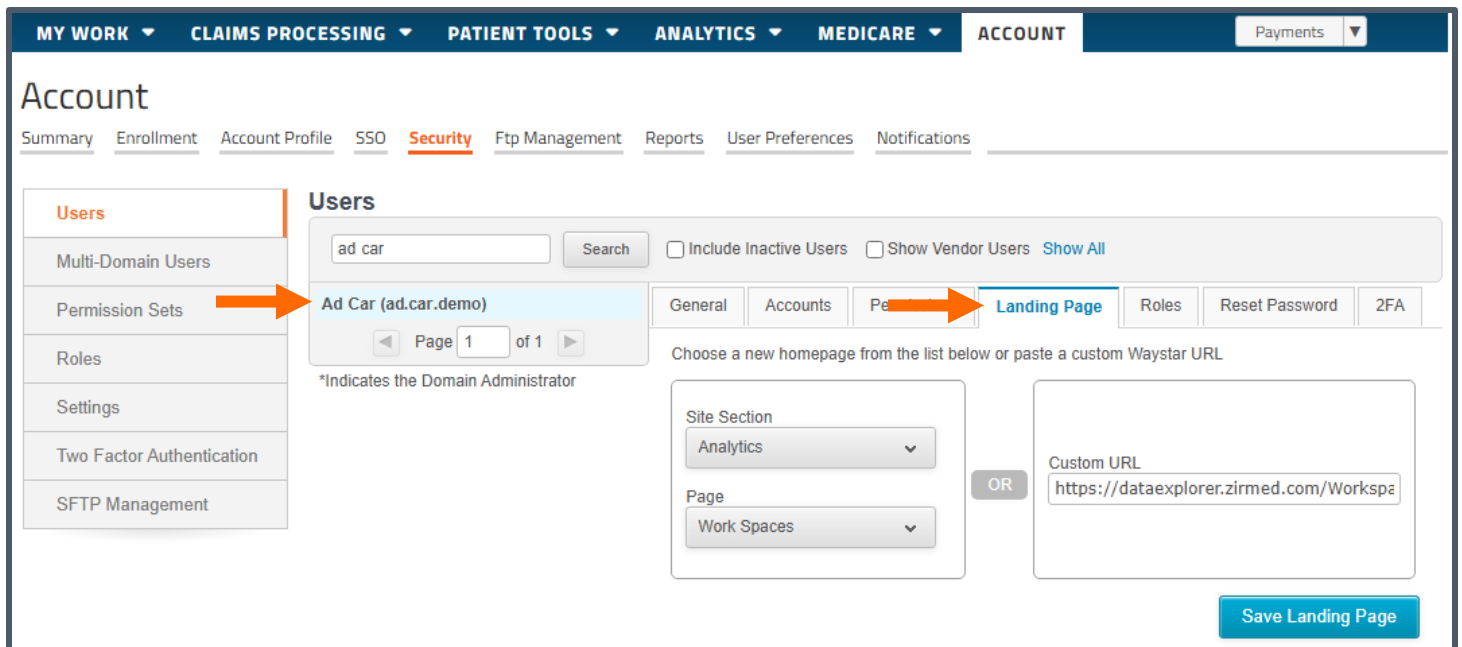
Using the Landing Page tab

This section explains how Domain Administrators and Security Managers can set a user's landing page when the user logs into the Waystar portal.

Note: The end user can set their default homepage by going to **ACCOUNT > User Preferences > Default Homepage**, as described in the "Customizing your User Preferences" article in the STC.

To set up a landing page:

1. To the right of the selected user, go to **ACCOUNT > Security > Users**.
2. Select a user.
3. Click the **Landing Page** tab.



The screenshot shows the 'Users' management interface. On the left is a sidebar with navigation links: Users, Multi-Domain Users, Permission Sets, Roles, Settings, Two Factor Authentication, and SFTP Management. An orange arrow points from 'Permission Sets' to the 'Users' section. The main area is titled 'Users' and contains a search bar with 'ad car' entered. Below the search bar, a table lists users, with 'Ad Car (ad.car.demo)' selected. An orange arrow points from the 'Ad Car' user entry to the 'Landing Page' tab in the user's profile. The 'Landing Page' tab is active and shows options to 'Choose a new homepage from the list below or paste a custom Waystar URL'. There are two dropdown menus: 'Site Section' (set to 'Analytics') and 'Page' (set to 'Work Spaces'). An 'OR' button is between these dropdowns and a 'Custom URL' field containing 'https://dataexplorer.zirmed.com/Workspa'. A 'Save Landing Page' button is at the bottom right.

4. Complete either of the following:
 - **Site Section and Page auto-select:**
 - Using the **Site Section** dropdown, you have the option of setting the default Homepage to a number of high-level Waystar screens, including **Professional Claims**, **Work Centers**, and more.
 - If the screen you selected in the Site Section dropdown has more specific pages to choose from, select the desired screen from the **Page** dropdown. For example, select the **Analytics** Site Section and the **Work Spaces** Page.
 - **Custom URL:** If you do not see the screen in one of the above dropdowns, use your browser and copy any Waystar URL and paste it in the **Custom URL** field.
5. When finished, click the **Save Landing Page** button.

The applied settings will appear the next time the user logs into Waystar.

Using the Roles tab

This section explains how to set a user's role or how to create a new role. In the Waystar portal, roles allow you to define accounts and permissions that you can then assign to users, who will then inherit those settings. For example, you can set up a Front Desk role that has access to certain accounts and requires certain permissions that you can then assign to one or more users.

Creating a new role

This section explains how Domain Administrators and Security Managers can create a new role. Once you create the role you can then assign it to users who will automatically inherit the role's accounts and permissions.

To create a new role:

1. Go to **ACCOUNT > Security > Roles**.
2. Click the **New Role** link.
A New Role entry area will open.
3. Enter the **Name** and **Description** of the new role.
4. Click the **Add Role** button.

The new role will display in the role list of the **ACCOUNT > Security > Users > Roles** tab

5. After the role is created, you can add accounts, permissions, and users to the role.

Assigning a role to multiple users

This section explains how Domain Administrators and Security Managers can set roles for multiple users. If a role does not exist, see the [Creating a new role](#) section.

To set roles for multiple users:

1. Go to **ACCOUNT > Security > Roles**.
2. From the list of roles on the left, select a role.
3. To the right of the selected role, click the **Users** tab.
4. Select one or more users.
5. Repeat as needed.

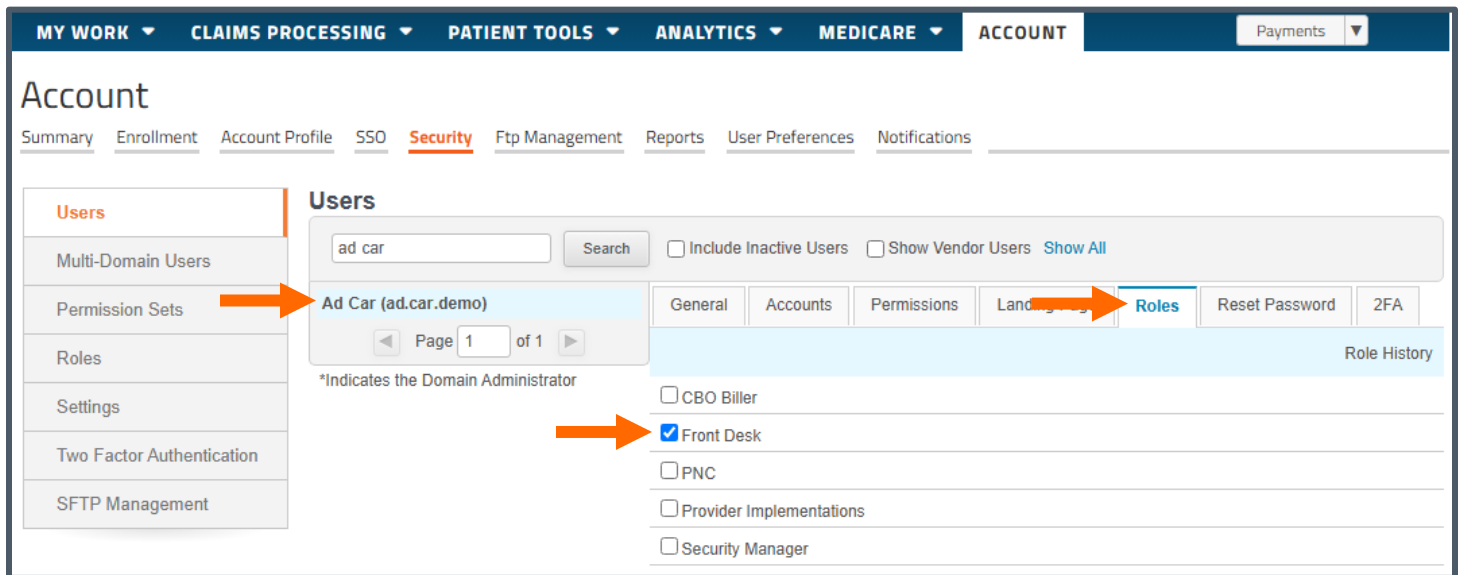
The screenshot shows the Waystar Account Security Roles page. The top navigation bar includes tabs for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT, and ADMIN. The ACCOUNT tab is selected, and the sub-tab is Security. The main content area is titled 'Roles' and contains a list of roles: AMD Role, CBO Biller, Front Desk, PNC, Provider Implementations, and Security Manager. The 'AMD Role' is selected. To the right of the roles list, there are tabs for General, Accounts, Payments, and Users. The 'Users' tab is selected. Below the tabs, there is a list of users with checkboxes for selection. The users listed are Ad Car, Ad Fum, Ad Young, Al Hu, Al Val, Al Cher, and Al Wore. The 'Ad Fum' checkbox is checked. An orange box highlights the 'Ad Fum' checkbox and the 'Al Val' and 'Al Cher' checkboxes. An orange arrow points from the 'Roles' menu item to the 'AMD Role' in the list. Another orange arrow points from the 'Users' tab to the 'Users' tab. A third orange arrow points to the 'Ad Fum' checkbox in the list of users.

Assigning a role to individual users

This section explains how Domain Administrators and Security Managers can set an individual user's role, which can include setting up designated users as Security Managers. If a role does not exist, see the [Creating a new role](#) section.

To set a user's role:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. To the right of the selected user, click the **Roles** tab.
4. Select the checkbox to give the user the role.
5. Repeat as needed.



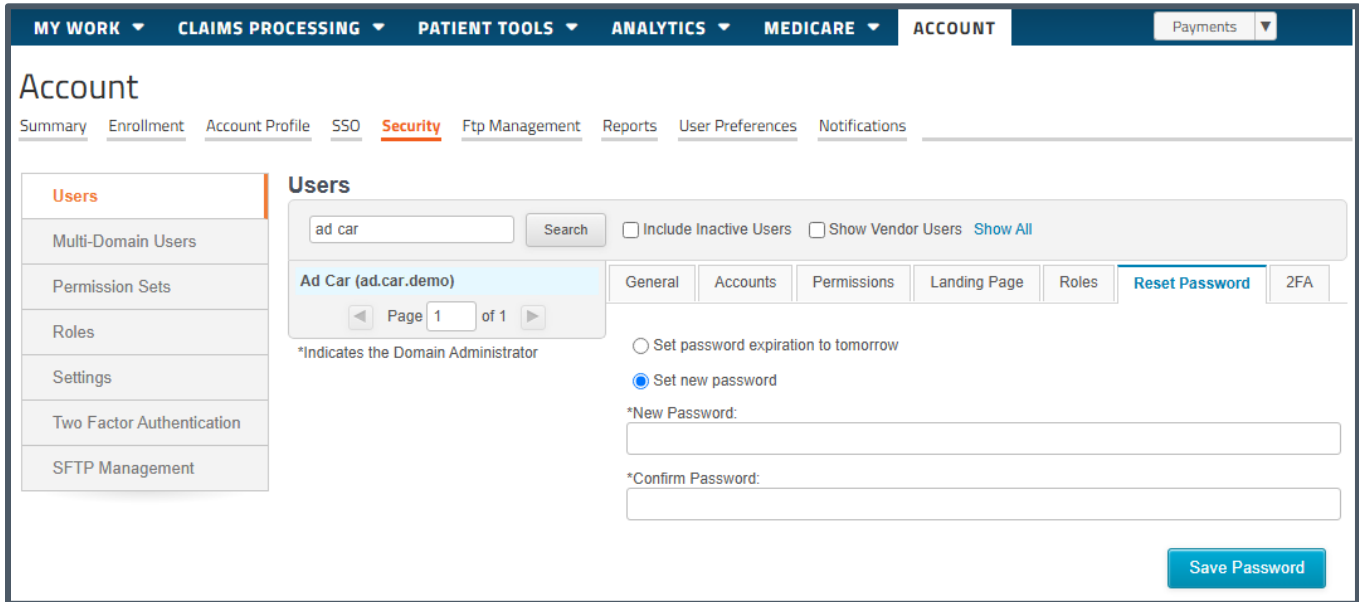
The screenshot displays the Waystar Account interface. The top navigation bar includes tabs for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is active, and a dropdown menu shows 'Payments'. Below the navigation bar, the 'Account' section is visible, with tabs for Summary, Enrollment, Account Profile, SSO, Security, Ftp Management, Reports, User Preferences, and Notifications. The 'Security' tab is selected. On the left, a sidebar menu lists 'Users', 'Multi-Domain Users', 'Permission Sets', 'Roles', 'Settings', 'Two Factor Authentication', and 'SFTP Management'. An orange arrow points from 'Permission Sets' to the 'Users' section. The 'Users' section shows a search bar with 'ad car' and a 'Search' button. Below the search bar, a table lists users, with 'Ad Car (ad.car.demo)' selected. An orange arrow points from the 'Ad Car (ad.car.demo)' row to the 'Roles' tab. The 'Roles' tab is active, showing a list of roles with checkboxes: CBO Biller, Front Desk (checked), PNC, Provider Implementations, and Security Manager. An orange arrow points from the 'Front Desk' checkbox to the 'Roles' tab. The 'Roles' tab also includes a 'Role History' section.

Using the Reset Password tab

This section explains how Domain Administrators and Security Managers can update/reset passwords for other users (but not for themselves). For end users to update their own passwords, they would go to the Waystar portal login screen and click the **Forgot your username or password?** link.

To reset a password:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. To the right of the selected user, click the **Reset Password** tab.



The screenshot shows the Waystar Account interface. The top navigation bar includes tabs for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is active, and a dropdown menu shows 'Payments'. Below the navigation bar, the 'Account' section is visible with sub-tabs: Summary, Enrollment, Account Profile, SSO, Security (highlighted), Ftp Management, Reports, User Preferences, and Notifications. On the left, a sidebar menu lists: Users (highlighted), Multi-Domain Users, Permission Sets, Roles, Settings, Two Factor Authentication, and SFTP Management. The main content area is titled 'Users' and contains a search bar with 'ad car' entered. Below the search bar, a table lists users, with 'Ad Car (ad.car.demo)' selected. To the right of the selected user, there are tabs: General, Accounts, Permissions, Landing Page, Roles, Reset Password (highlighted), and 2FA. The 'Reset Password' tab contains two radio buttons: 'Set password expiration to tomorrow' (unselected) and 'Set new password' (selected). Below these are two text input fields labeled '*New Password:' and '*Confirm Password:'. A 'Save Password' button is located at the bottom right of the form.

4. Complete one of the following as appropriate:
 - **Set password expiration to tomorrow:** Select this to force a user's password to expire the following day. The system will force the user to change their password when they log in.
 - **Set new password:** Select this to manually enter a **New Password** and **Confirm Password** for the user. A new password must adhere to the following parameters:
 - Contains at least 15 characters
 - Contains at least one number
 - Contains at least one uppercase AND one lowercase character
 - Contains at least one special character
 - Cannot contain any of the following special characters `< > * % & : \ ?`
 - Cannot contain the user's first name, last name, or Waystar username
 - Cannot have consecutively repeating characters
 - Cannot repeat previous 24 passwords
 - Cannot be a commonly used password.

For additional information, see the [Setting password options](#) section.

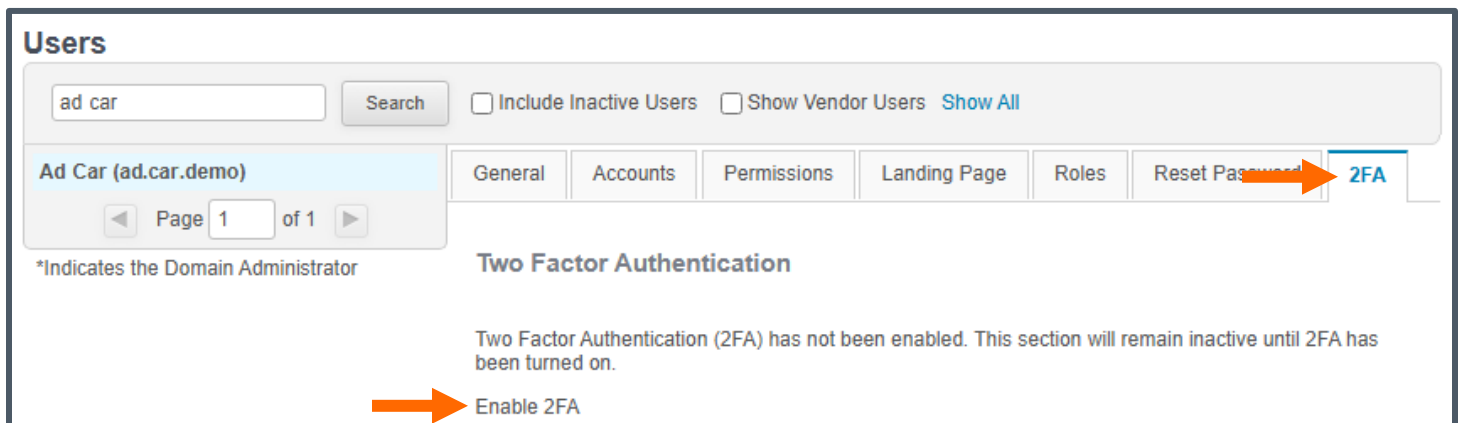
5. Click the **Save Password** button.

Using the 2FA tab

This section explains how Domain Administrators and Security Managers can use the 2FA (two-factor authentication) tab. When two-factor authentication is enabled for your organization (see the [Enabling \(requiring\) two-factor authentication](#) section), you can use this tab to send one-time codes to users who have lost access to their Waystar account.

To use the 2FA tab:

1. Go to **ACCOUNT > Security > Users**.
2. Select a user.
3. To the right of the selected user, click the **2FA** tab.
4. Do the following as appropriate:
 - If two-factor authentication is disabled for your organization, the tab will display a link that will take you to the Two Factor Authentication screen where you can enable it. See the [Enabling \(requiring\) two-factor authentication](#) section.



The screenshot shows the 'Users' management interface. At the top, there is a search bar with 'ad car' entered and a 'Search' button. Below the search bar, there are checkboxes for 'Include Inactive Users' and 'Show Vendor Users', and a 'Show All' link. A user named 'Ad Car (ad.car.demo)' is selected, and the '2FA' tab is active. The '2FA' tab shows a message: 'Two Factor Authentication (2FA) has not been enabled. This section will remain inactive until 2FA has been turned on.' Below this message is a button labeled 'Enable 2FA' with an orange arrow pointing to it. The interface also includes a 'Page 1 of 1' indicator and a note: '*Indicates the Domain Administrator'.

- If two-factor authentication is enabled and a user loses access to their Waystar account, you can do either of the following:
 - **Generate code for this user:** Will generate a code and display it on the screen.

Users

☒ Include Inactive Users
 ☐ Show Vendor Users
 [Show All](#)

[+ New User](#)

*Demo Admin (demodomainadmin)

Demo External User (demoexternaluser) [Inactive]

Demo Security Manager (demosecuritymanager) [Inactive]

tim tester (timtestuser) [Inactive]

Page 1 of 1

*Indicates the Domain Administrator

General

Accounts

Permissions

Landing Page

Roles

Reset Password

2FA

Two Factor Authentication

If a user loses access to their Waystar account, you have the option to send them a security code that will grant them 1-time access into Waystar. At this point they should change their two factor authentication settings so they can avoid issues accessing their account in the future.

Temporary Code:

345127

- **Send code to user:** Will email or text the code to the user, which you can select from the screen, so that they can receive the code and access the Waystar portal.

Users

☒ Include Inactive Users
 ☐ Show Vendor Users
 [Show All](#)

[+ New User](#)

*Demo Admin (demodomainadmin)

Demo External User (demoexternaluser) [Inactive]

Demo Security Manager (demosecuritymanager) [Inactive]

tim tester (timtestuser) [Inactive]

Page 1 of 1

*Indicates the Domain Administrator

General

Accounts

Permissions

Landing Page

Roles

Reset Password

2FA

Two Factor Authentication

If a user loses access to their Waystar account, you have the option to send them a security code that will grant them 1-time access into Waystar. At this point they should change their two factor authentication settings so they can avoid issues accessing their account in the future.

Select a method from below:

☐ Email on File *****maluser@test.com
 ☐ Manual Entry

Phone Number

Setting security

This section explains how a Domain Administrator can set up password and IP options.

Setting password options

This section explains how a Domain Administrator can set up allowed password rotation and auto-deactivation.

Note: Security Managers cannot update this screen.

To set password options:

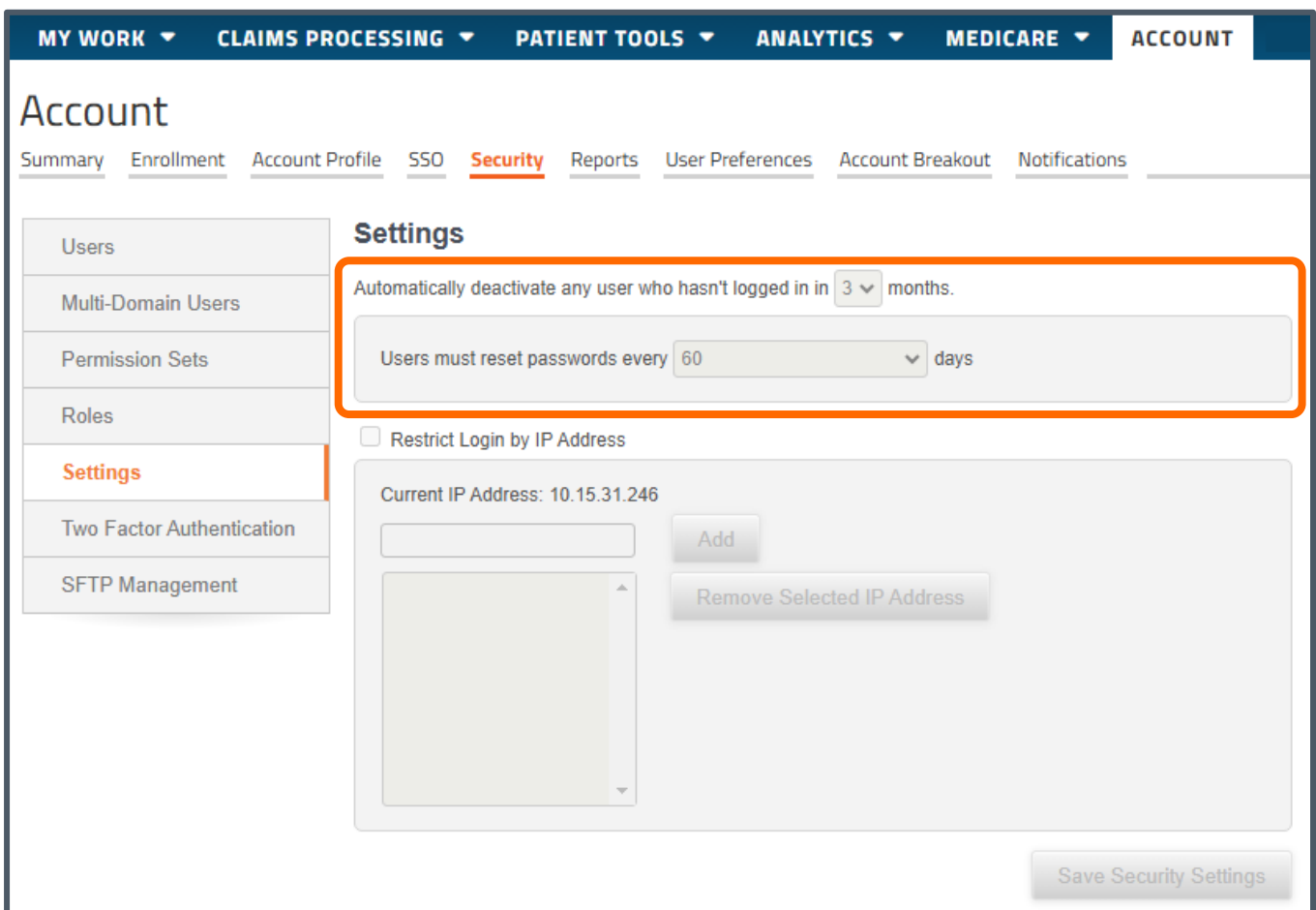
1. Go to **ACCOUNT > Security > Settings**.

The Settings screen will open.

2. From the dropdown boxes, select:

- **Auto-deactivation:** Set the **Automatically deactivate any user who hasn't logged in in X months** field using the dropdown. You can select from 1 to 3 months.
- **Change frequency:** Set the **Users must reset passwords every X days** field using the dropdown. You can select from 30 to 60 days.

3. When finished, click the **Save Security Settings** button.



MY WORK ▾ CLAIMS PROCESSING ▾ PATIENT TOOLS ▾ ANALYTICS ▾ MEDICARE ▾ ACCOUNT

Account

Summary Enrollment Account Profile SSO **Security** Reports User Preferences Account Breakout Notifications

Users

Multi-Domain Users

Permission Sets

Roles

Settings

Two Factor Authentication

SFTP Management

Settings

Automatically deactivate any user who hasn't logged in in **3** months.

Users must reset passwords every **60** days

☐ Restrict Login by IP Address

Current IP Address: 10.15.31.246

Add

Remove Selected IP Address

Save Security Settings

Working with IP addresses

This section explains how a Domain Administrator can enable and restrict system access to the specified IP address(es) and how to remove an IP address restriction.

Note: Security Managers cannot update this screen.

Restricting login by IP address

This section explains how a Domain Administrator can restrict anyone logging into your system to one or more specific IP addresses, meaning the user must be using those specified IP address(es) to log into your system.

Note: Security Managers cannot update this screen.

To restrict login by IP address:

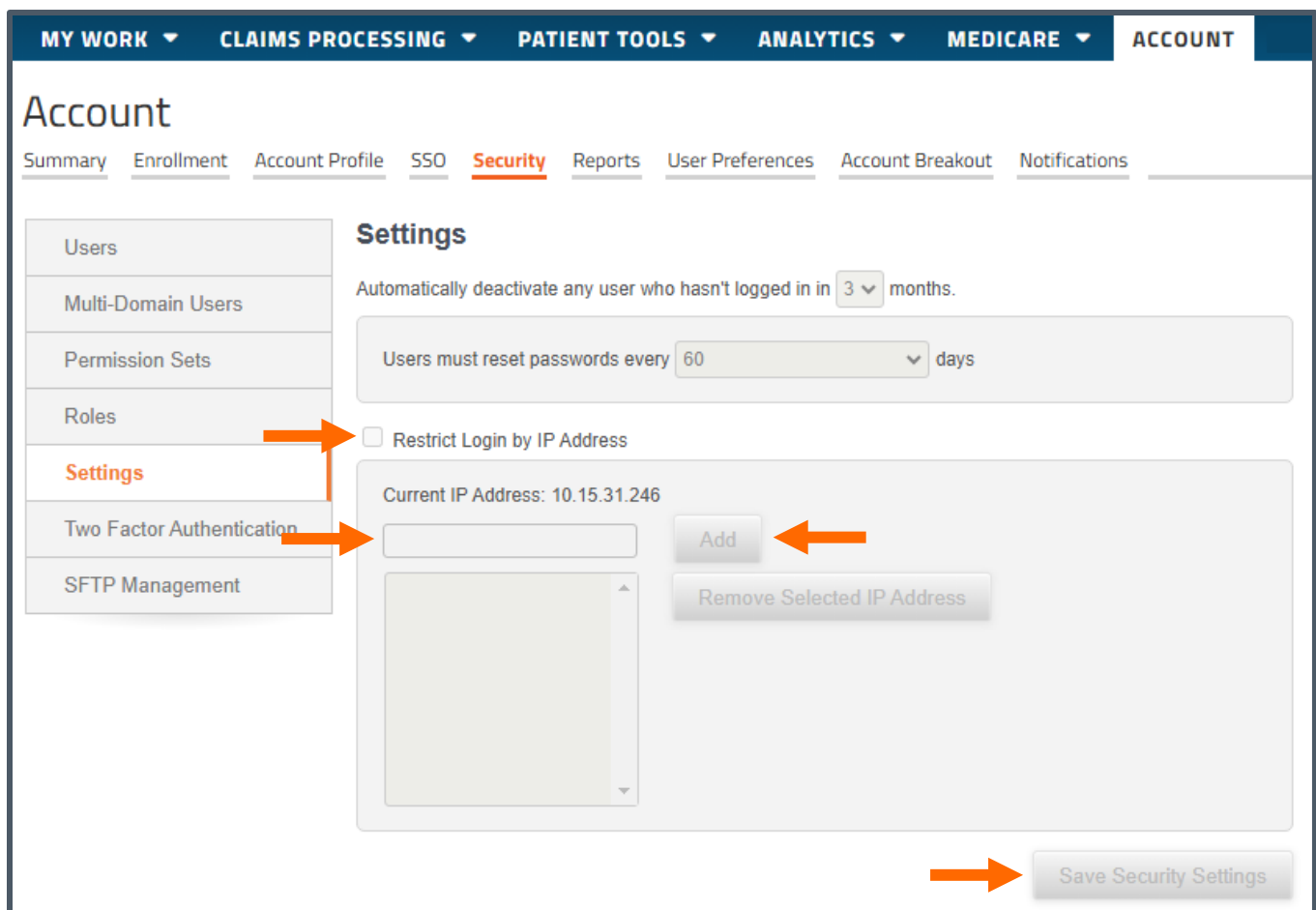
1. Go to **ACCOUNT > Security > Settings**.

The Settings screen will open.

2. Select the **Restrict Login by IP Address** checkbox.
3. Enter the IP address from which a login is allowed.

Note: To find a user's IP address, run the [System Access Report](#).

4. Click the **Add** button.
5. When finished, click the **Save Security Settings** button.



The screenshot shows the 'Account' page with the 'Security' tab selected. In the left sidebar, the 'Settings' option is highlighted with an orange arrow. The main content area is titled 'Settings' and includes a checkbox for 'Restrict Login by IP Address', which is also pointed to by an orange arrow. Below this checkbox, there is a text input field for 'Current IP Address' (showing 10.15.31.246), an 'Add' button (pointed to by an orange arrow), and a 'Remove Selected IP Address' button. At the bottom right, a 'Save Security Settings' button is pointed to by an orange arrow. Other settings visible include 'Automatically deactivate any user who hasn't logged in in 3 months' and 'Users must reset passwords every 60 days'.

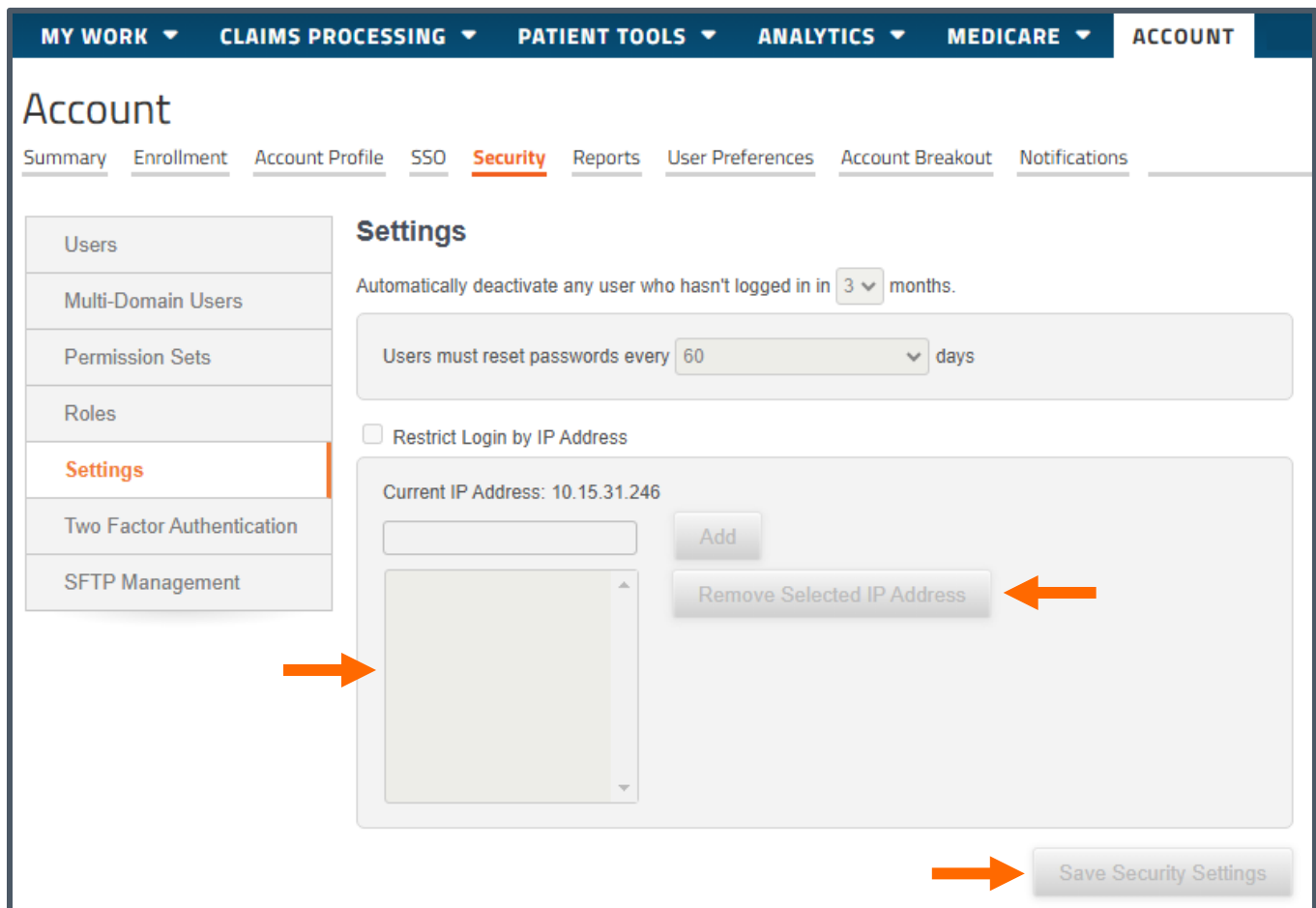
Removing an IP address restriction

This section explains how a Domain Administrator can remove an IP address restriction.

Note: Security Managers cannot update this screen.

To remove an IP address restriction:

1. Go to **ACCOUNT > Security > Settings**.
The Settings screen will open.
2. Select the **IP address** in the list of accepted addresses.
3. Click the **Remove Selected IP Address** button.
4. When finished, click the **Save Security Settings** button.



The screenshot shows the 'Account' page with the 'Security' tab selected. The 'Settings' section is active, displaying options for user deactivation and password resets. The 'Restrict Login by IP Address' checkbox is unchecked. Below it, the 'Current IP Address' is listed as 10.15.31.246. A list of accepted IP addresses is shown with an 'Add' button. The 'Remove Selected IP Address' button is highlighted with an orange arrow. The 'Save Security Settings' button at the bottom right is also highlighted with an orange arrow. The left sidebar contains a menu with 'Settings' highlighted in orange.

Account

Summary Enrollment Account Profile SSO **Security** Reports User Preferences Account Breakout Notifications

Settings

Automatically deactivate any user who hasn't logged in in 3 months.

Users must reset passwords every 60 days

☐ Restrict Login by IP Address

Current IP Address: 10.15.31.246

Add

Remove Selected IP Address

Save Security Settings

Working with Permission Sets

Overview

Permission sets allow your organization to select and save a specific "set" of permissions that you want to grant to your users. Waystar provides the following permission sets:

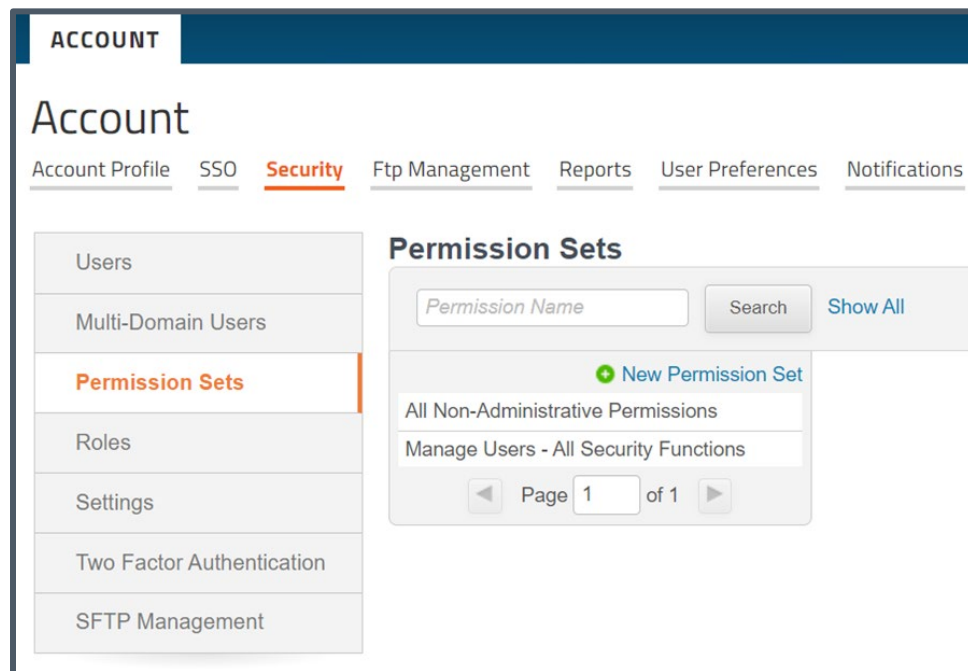
- **All Non-Administrative Permissions:** This permission set would give the user all permissions to every solution within the domain that fall outside those permissions for domain administrators and security managers.
- **Manage Users:** This permission set is for domain administrators and security managers, providing them access to all the screens necessary for them to manage their users.

Waystar recommends creating your own custom permission sets. This is because the All Non-Administrative Permissions set is most likely too broad for your non-admin users and you might have permissions outside of the Manage Users permission set that you want manager or admin users to have.

You can create as many permission sets as necessary, defining them as broadly or narrowly as you want. Once created, you would then use your custom sets to assign permissions to your users. For example:

- You might want a different permission set for your back-office users compared to your patient access users.
- You might want a permission set for each individual Waystar solution that you license, such as a permission set Patient Tools.

To view permission sets, go to **ACCOUNT > Security > Permission Sets**.



Creating a custom permission set

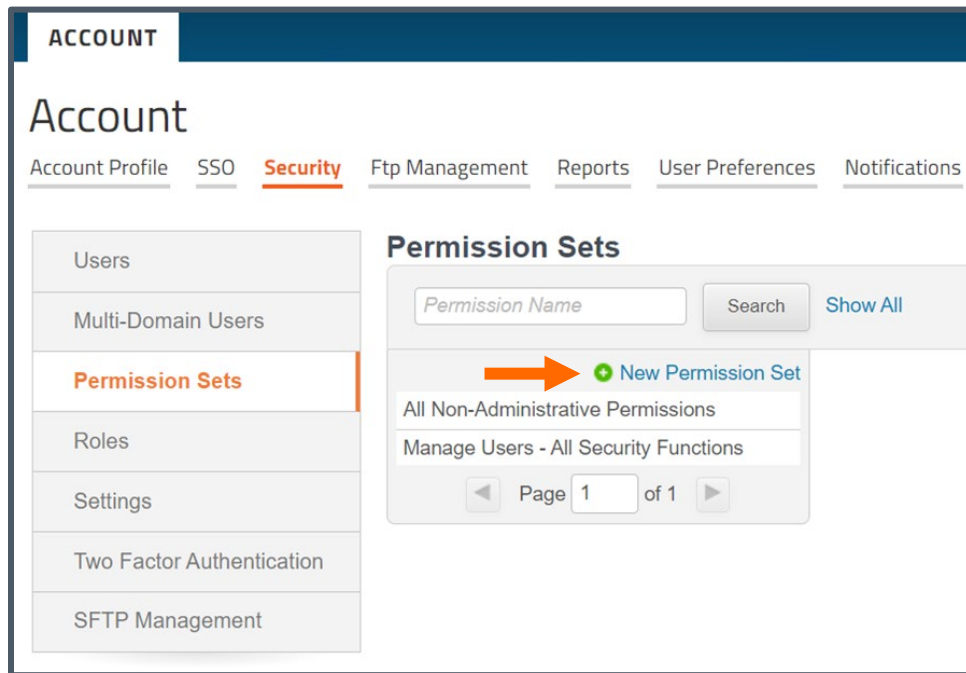
This section explains how Domain Administrators and Security Managers can create a custom permission set for your organization.

To create a custom permission set:

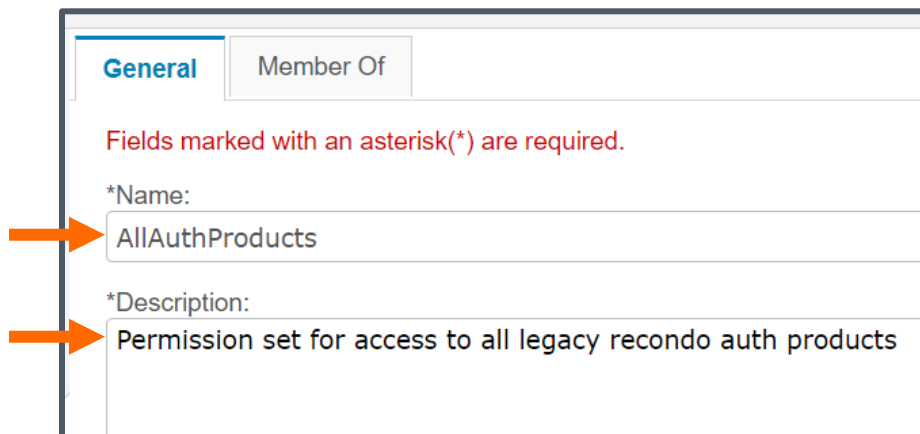
1. Go to **ACCOUNT > Security > Permission Sets**.

The Permission Sets screen will open.

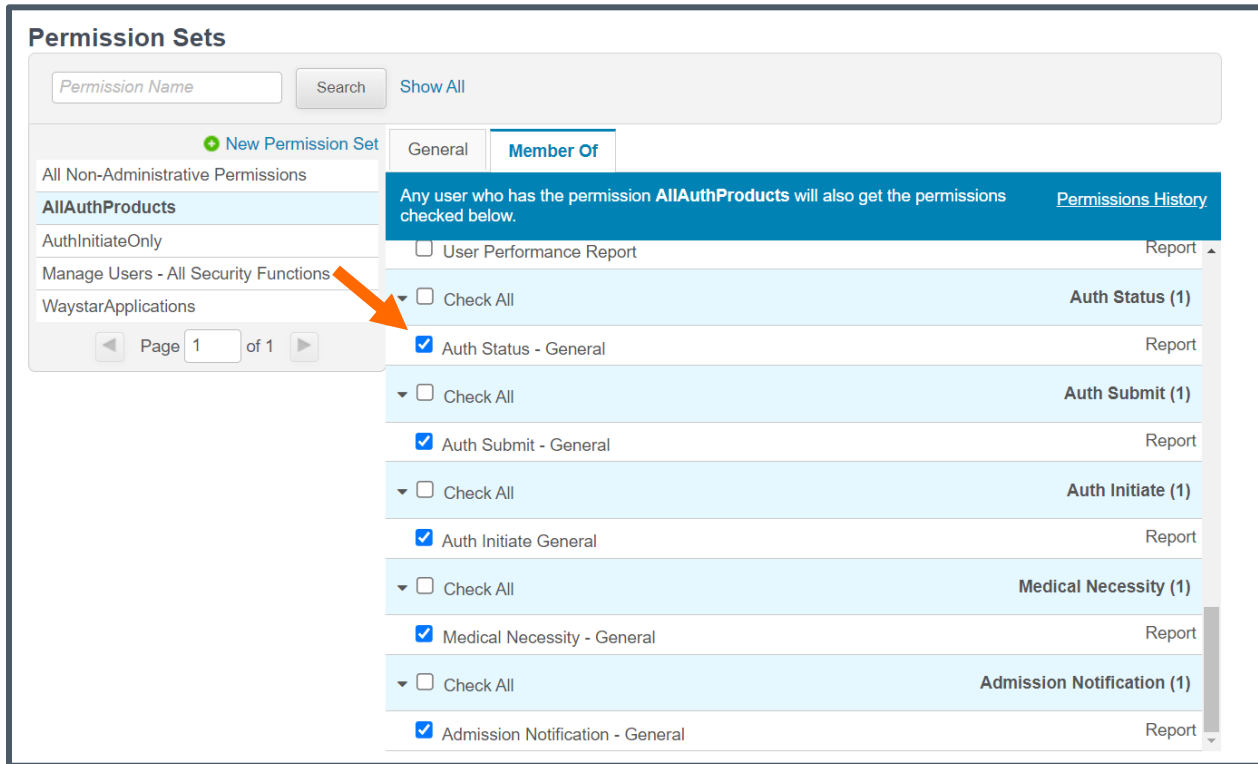
2. Click the **New Permission Set** link.



3. From the General tab that will open, enter the permission set **Name** and **Description**.

The screenshot shows the 'General' tab of the 'New Permission Set' form. The 'Member Of' dropdown is set to 'AllAuthProducts'. The form has two required fields: '*Name:' and '*Description:'. The 'Name' field contains 'AllAuthProducts' and the 'Description' field contains 'Permission set for access to all legacy recondo auth products'. Orange arrows point to both fields. A red message at the top states: 'Fields marked with an asterisk(*) are required.'

- Click the checkbox to view the permission set in either the **simple view**, **advanced view**, or **both**.
- Click the **Member Of** tab.
- Select the checkboxes of all the permissions you want the new set to have.



Permission Sets

Permission Name Search Show All

+ New Permission Set

All Non-Administrative Permissions

AllAuthProducts

AuthInitiateOnly

Manage Users - All Security Functions

WaystarApplications

Page 1 of 1

General Member Of

Any user who has the permission AllAuthProducts will also get the permissions checked below. [Permissions History](#)

<input type="checkbox"/> User Performance Report	Report
<input type="checkbox"/> Check All	Auth Status (1)
<input checked="" type="checkbox"/> Auth Status - General	Report
<input type="checkbox"/> Check All	Auth Submit (1)
<input checked="" type="checkbox"/> Auth Submit - General	Report
<input type="checkbox"/> Check All	Auth Initiate (1)
<input checked="" type="checkbox"/> Auth Initiate General	Report
<input type="checkbox"/> Check All	Medical Necessity (1)
<input checked="" type="checkbox"/> Medical Necessity - General	Report
<input type="checkbox"/> Check All	Admission Notification (1)
<input checked="" type="checkbox"/> Admission Notification - General	Report

- To apply your changes, go back to the **General** tab and click the **Save** button.

Edit an existing permission set

This section explains how Domain Administrators and Security Managers can edit your organization's existing permission sets to add or remove permissions from the set.

IMPORTANT: If a permission set is edited or deleted, all users who have this permission set are affected.

To edit an existing permission set:

- Go to **ACCOUNT > Security > Permission Sets**.
The Permission Sets screen will open.
- Locate the permission set name you want to edit. You can use the search field at the top of the screen.
- From the list of permission set names, click the one you want to edit.
- Click the **Member Of** tab.
- Select or clear (unselect) the checkboxes of the appropriate permissions.
- To save the changes, go back to the **General** tab and click the **Update Permissions Set** button.

Enabling and using two-factor authentication

This section explains how a Domain Administrator can enable two-factor authentication, which lessens the risk of malicious attempts to access a user's account. When two-factor authentication is enabled, a user will be required to provide the following forms of identification when logging into the Waystar portal:

- Their username and password
- An authentication code that the user will be prompted to request and then receive from Waystar (as explained in this section).

Enabling (requiring) two-factor authentication

This section explains how a Domain Administrator can enable two-factor authentication.

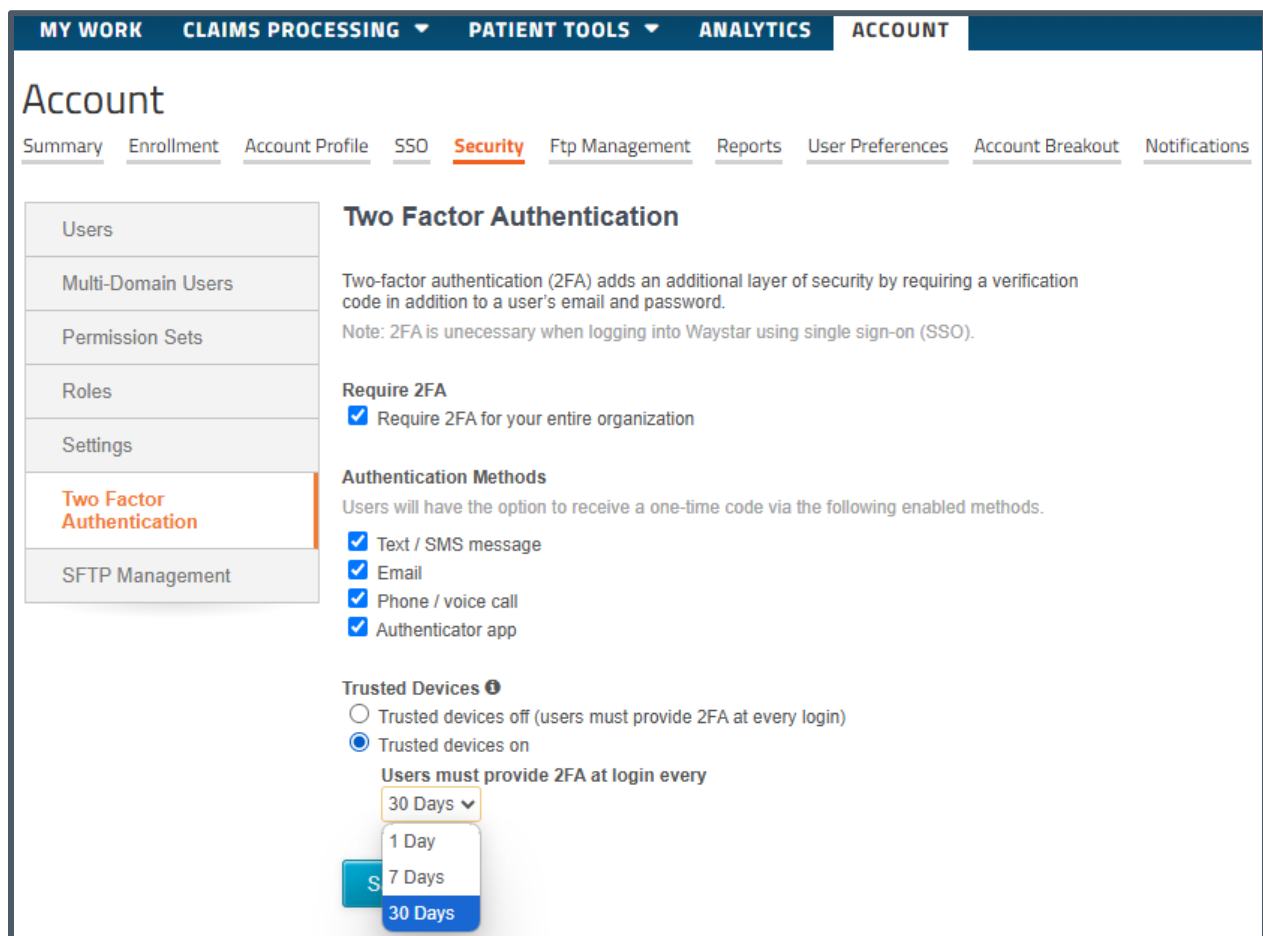
IMPORTANT:

- While it is optional for you to require two-factor authentication for your organization, if you enable this option, ***you cannot disable it***.
- Security Managers cannot update this screen.

To enable two-factor authentication for your organization:

1. Go to **ACCOUNT > Security > Two Factor Authentication**.

The Two Factor Authentication screen will open.



The screenshot shows the 'Two Factor Authentication' settings page within the Waystar portal. The top navigation bar includes 'MY WORK', 'CLAIMS PROCESSING', 'PATIENT TOOLS', 'ANALYTICS', and 'ACCOUNT'. The 'ACCOUNT' section is active, and the 'Security' tab is selected. The left sidebar lists various account management options, with 'Two Factor Authentication' highlighted. The main content area is titled 'Two Factor Authentication' and includes a description of 2FA, a note about SSO, and settings for requiring 2FA and enabling authentication methods. The 'Require 2FA' checkbox is checked. Under 'Authentication Methods', four options are checked: Text / SMS message, Email, Phone / voice call, and Authenticator app. The 'Trusted Devices' section shows 'Trusted devices on' selected, with a dropdown menu for 'Users must provide 2FA at login every' showing options for 1 Day, 7 Days, and 30 Days.

Account

Summary Enrollment Account Profile SSO **Security** Ftp Management Reports User Preferences Account Breakout Notifications

Two Factor Authentication

Two-factor authentication (2FA) adds an additional layer of security by requiring a verification code in addition to a user's email and password.

Note: 2FA is unnecessary when logging into Waystar using single sign-on (SSO).

Require 2FA

☒ Require 2FA for your entire organization

Authentication Methods

Users will have the option to receive a one-time code via the following enabled methods.

☒ Text / SMS message

☒ Email

☒ Phone / voice call

☒ Authenticator app

Trusted Devices

☐ Trusted devices off (users must provide 2FA at every login)

☒ Trusted devices on

Users must provide 2FA at login every

30 Days

1 Day

7 Days

30 Days

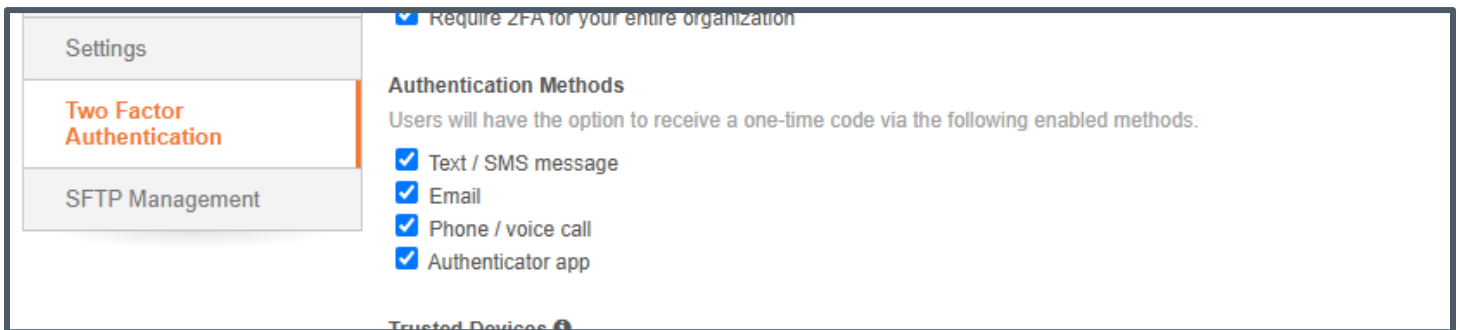
2. If you want to require two-factor authentication for your organization, select the **Require 2FA for your entire organization** checkbox. While requiring this for your organization is optional, if you do enable this option, **you cannot disable it**.

3. To set the **Authentication Methods** that you want your users to have access to:

a. Select one or more of the following methods:

- Text/SMS message
- Email
- Phone/voice call
- Authenticator app

The selected methods will appear on the User Preferences > Two Factor Authentication screen as explained in the next step.



Settings

- Two Factor Authentication**
- SFTP Management

☒ Require 2FA for your entire organization

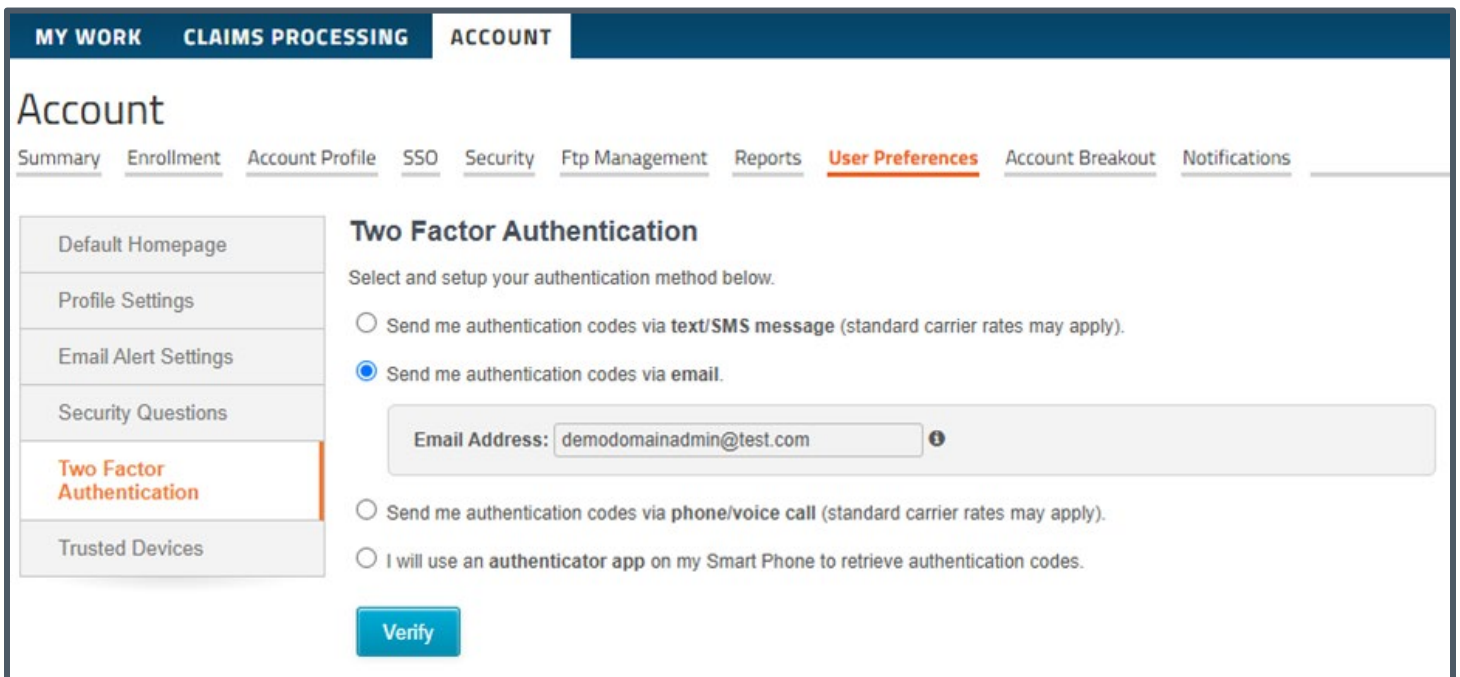
Authentication Methods

Users will have the option to receive a one-time code via the following enabled methods.

- ☒ Text / SMS message
- ☒ Email
- ☒ Phone / voice call
- ☒ Authenticator app

Trusted Devices

b. The user needs to go to **ACCOUNT > User Preferences > Two Factor Authentication** to select one method they want to use.



MY WORK CLAIMS PROCESSING ACCOUNT

Account

Summary Enrollment Account Profile SSO Security Ftp Management Reports **User Preferences** Account Breakout Notifications

Two Factor Authentication

Select and setup your authentication method below.

☐ Send me authentication codes via **text/SMS message** (standard carrier rates may apply).

☒ Send me authentication codes via **email**.

Email Address:

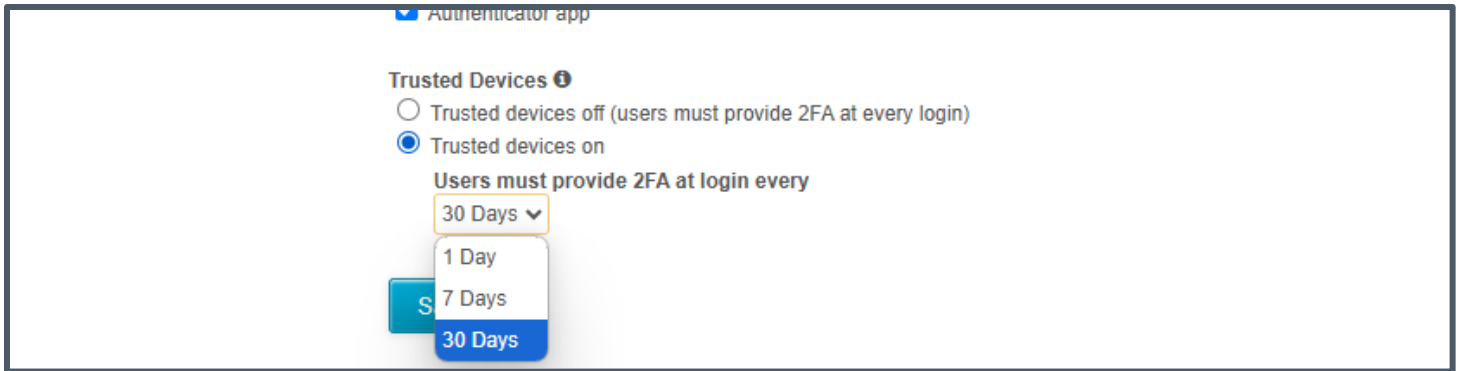
☐ Send me authentication codes via **phone/voice call** (standard carrier rates may apply).

☐ I will use an **authenticator app** on my Smart Phone to retrieve authentication codes.

Verify

4. To set how you want your users to designate **Trusted Devices**, you have the following options:

- **Trusted devices off:** Users must use two-factor authentication every time they log in.
- **Trusted devices on:** From the dropdown, select how often a user must use two-factor authentication if they have designated a trusted device.



Trusted Devices ⓘ

☐ Trusted devices off (users must provide 2FA at every login)

☒ Trusted devices on

Users must provide 2FA at login every

30 Days ▼

1 Day

7 Days

30 Days

5. When finished making your two-factor authentication selections, click the **Save** button.

When enabled, all users in your organization will have to use two-factor authentication when logging into the Waystar portal, as explained in the [Using two-factor authentication](#) section.

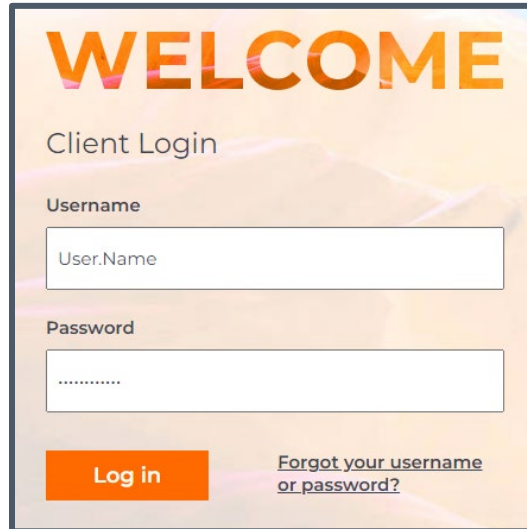
Using two-factor authentication

This section explains how an end-user interacts with two-factor authentication.

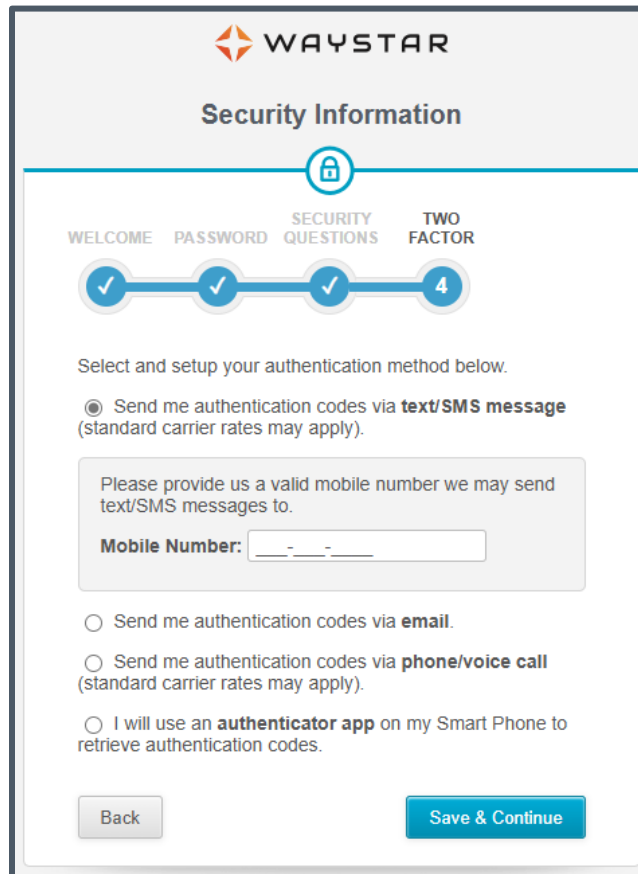
IMPORTANT: Your organization must [enable two-factor authentication](#) for it to appear for your users.

To use two-factor authentication:

1. On the Waystar portal's login screen, the user provides their username and password, and then clicks the **Log In** button.

The image shows the 'WELCOME Client Login' screen. It features a large orange 'WELCOME' header. Below it, the text 'Client Login' is displayed. There are two input fields: 'Username' with the placeholder 'User.Name' and 'Password' with a masked password '.....'. At the bottom left is an orange 'Log in' button. At the bottom right is a link that says 'Forgot your username or password?'.

The initial Two Factor Authentication screen will open.

The image shows the 'WAYSTAR Security Information' screen. At the top is the Waystar logo and the title 'Security Information'. Below this is a progress bar with four steps: 'WELCOME', 'PASSWORD', 'SECURITY QUESTIONS', and 'TWO FACTOR'. The first three steps are marked with checkmarks, and the fourth step is marked with a '4'. Below the progress bar, the text 'Select and setup your authentication method below.' is displayed. There are three radio button options: 'Send me authentication codes via text/SMS message (standard carrier rates may apply).', 'Send me authentication codes via email.', and 'Send me authentication codes via phone/voice call (standard carrier rates may apply).'. The first option is selected. Below the first option is a text input field for 'Mobile Number' with a placeholder '____-____-____'. At the bottom left is a 'Back' button, and at the bottom right is a 'Save & Continue' button.

2. The user selects which method of authentication they want to use:

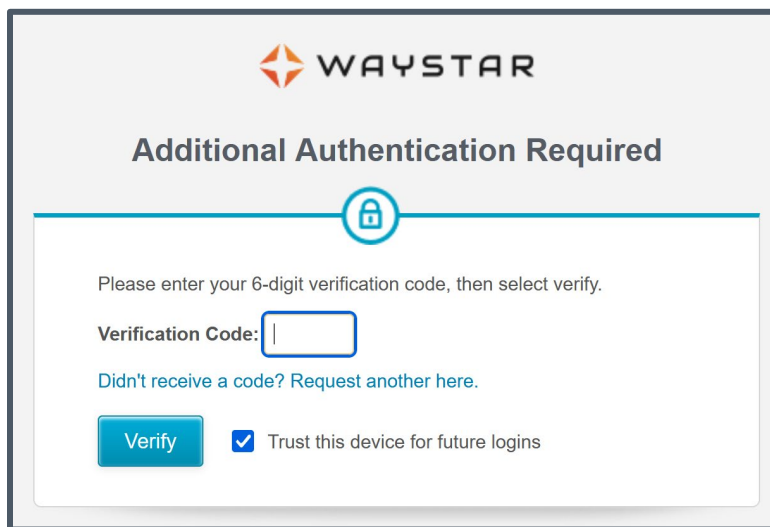
- Text/SMS message
- Email
- Phone/Voice Call
- Authenticator App

Note: The user can also set this option from ACCOUNT > User Preferences > Two Factor Authentication.

3. The user then clicks the **VERIFY** button.

The user will receive the authentication code and the subsequent Two Factor Authentication screen will open.

Note: If the user did not receive the requested code, they can request another by clicking the link beneath the Verification Code field.



4. In the **Verification Code** field, the user enters the code provided to them by Waystar.

5. *Optional.* If the device they're using is secure, they can select the **Trust this device for future logins** checkbox, which will then bypass two-factor authentication.

6. The user clicks the **Verify** button.

The Waystar portal will open to the user's default homepage.

Note: The end user can set their default homepage by going to **ACCOUNT > User Preferences > Default Homepage**, as described in the "Customizing your User Preferences" article in the STC.

Using the System Access Report

This section explains how Domain Administrators and Security Managers can customize, view, and/or print the System Access Report. The report shows all active or inactive users who have accessed your domain within a specified date range.

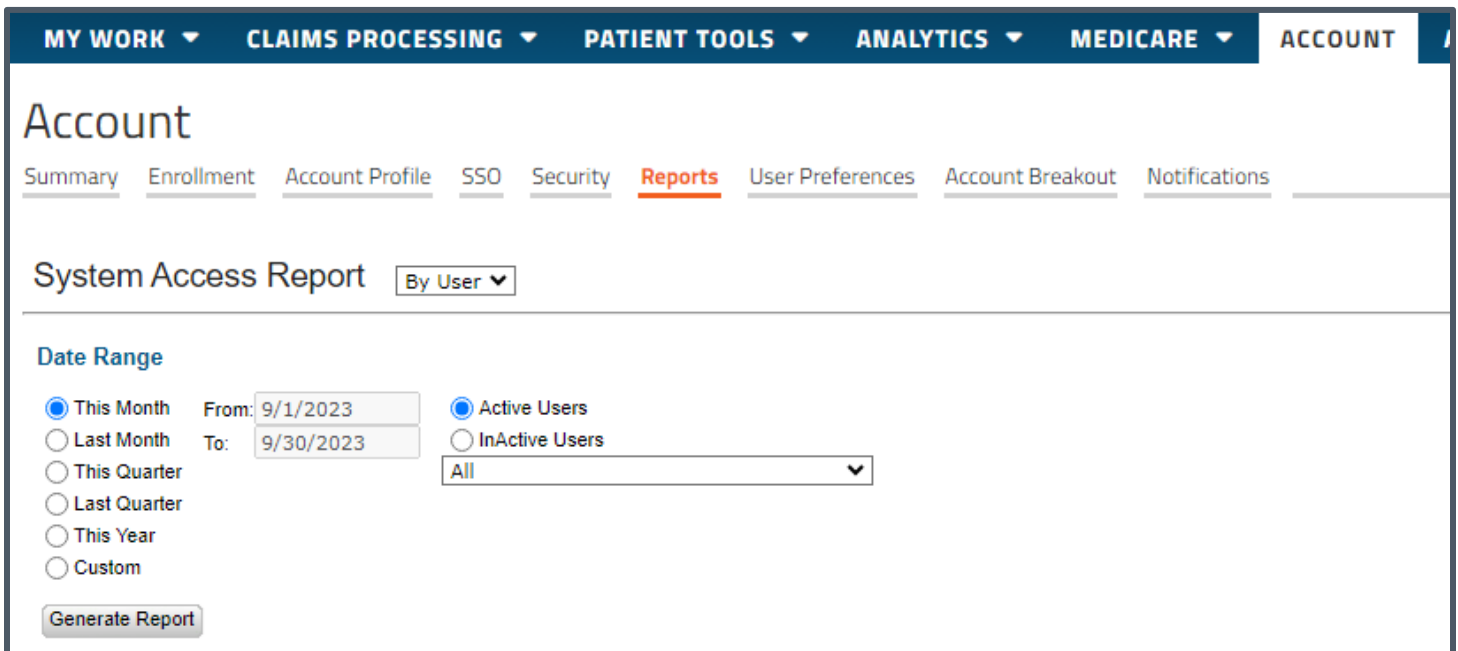
To use the System Access Report:

1. Go to **ACCOUNT > Reports**.
2. Click the **System Access Report** link.

The System Access Report screen will open.

3. Use any of the following filter options:

- To sort the report by username or date, use the dropdown at the top of the screen to select **By User** or **By Date**.
- To generate user information for the selected time period, select the appropriate date range in the **Date Range** area.
- To show users in the following dropdown who can log into your domain or users who have been deactivated, select either the **Active Users** or **InActive Users** radio button.
- To generate user information for a specific user, use the dropdown below the radio buttons to select the appropriate name (select **All** to see all active or inactive users).



4. After applying all desired filters, click the **Generate Report** button.

If data is available for the selected filters, the report will display on the screen.

Revision log

Date	Description	Version
June 2025	<ul style="list-style-type: none"> Added the “Hiding the Support and Training Center link” section under the “Using the General tab” section Updated the “Enabling (requiring) two-factor authentication” section 	6
February 2025	Reviewed and updated the guide throughout	5