



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.

The screenshot shows the Waystar portal interface. At the top, there is a navigation bar with tabs: MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is highlighted. Below the navigation bar, the word "Account" is displayed. A secondary navigation bar below "Account" includes links: Summary, Enrollment, Account Profile, SSO, Security (which is underlined in red), Reports, User Preferences, Account Breakout, and Notifications. On the left side, there is a sidebar titled "Users" containing links for Multi-Domain Users, Permission Sets, Roles, Settings, Two Factor Authentication, and SFTP Management. The main content area is titled "Users" and contains a list of user names. At the top of this list is a button labeled "+ New User". The user names listed are: 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), and Am Clar (am.clar.demo). Below the list is a pagination control showing "Page 1 of 17". At the bottom of the main content area, there is a note: "*Indicates the Domain Administrator".

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 shows the Waystar Health user management interface. At the top, there is a navigation bar with tabs: MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is highlighted. Below the navigation bar, the word "Account" is displayed. A secondary navigation bar below the main one includes: Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in orange), Reports, User Preferences, Account Breakout, and Notifications. On the left side, there is a sidebar titled "Users" with links: 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 the text "ad car", a "Search" button, and two checkboxes: "Include Inactive Users" and "Show Vendor Users". Below the search bar, a "New User" button is visible. A list of users is shown, with "Ad Car (ad.car.demo)" listed as the first item. At the bottom of the list, there is a pagination control showing "Page 1 of 1". A small 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.

The screenshot shows the Waystar portal's 'Account' section with the 'Users' tab selected. On the left, there is a sidebar with links: 'Multi-Domain Users', 'Permission Sets' (which has an orange arrow pointing to it), 'Roles', 'Settings', 'Two Factor Authentication', and 'SFTP Management'. The main area is titled 'Users' and shows a search bar with '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 table lists a single user: 'Ad Car (ad.car.demo)'. To the right of the table are tabs: General (highlighted with an orange box), Accounts, Permissions, Landing Page, Roles, Reset Password, and 2FA. Below these tabs is a note: '*Indicates the Domain Administrator'. The 'General' tab displays form fields for the user: 'User Name' (ad.car.demo), 'User ID: (Internal Use Only)' (111111), 'First Name' (Ad), 'Last Name' (Car), 'Email' (ad.car@star.com), 'Default Account' (America Healthcare Inc (729)), 'Pool Id' (Waystar Portal Standard Login Users), and checkboxes for 'Active' (checked), 'Force user to change password (setting will reset after user has changed their password)', and 'Clear users security questions (setting will reset after user has entered new security questions)'. At the bottom right is a 'Save General Settings' button.

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 portal interface with the following details:

- Top Navigation:** MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT (highlighted), ADMIN, Payments.
- Left Sidebar:** Summary, Enrollment, Account Profile, SSO, **Security** (highlighted), Reports, User Preferences, Account Breakout, Notifications.
- Current View:** Account - Security - Users.
- User List:** A table showing a list of users with names like Ad Car, Ad Fum, etc. An orange arrow points to the "New User" button at the top left of the list.
- Form Fields:** The "General" tab is selected. It contains fields for User Name, First Name, Last Name, Email, Default Account (set to America Healthcare Inc (729)), Pool Id (set to Waystar Portal Standard Login Users), Password, Confirm Password, Active checkbox (checked), Force user to change password (checkbox), and Clear users security questions (checkbox).
- Buttons:** Save General Settings button at the bottom right.

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.

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.



The screenshot shows a user profile edit form. In the 'Email' field, the text 'ad.car@waystar.com' is entered, and a small blue checkmark icon followed by the word 'Verified' is displayed to its left. Below the email field, there is a label 'Default Account'.

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 Health user management interface. The top navigation bar includes links for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT (which is selected), and Payments. The main page title is "Account". Below the title, there are tabs for Summary, Enrollment, Account Profile, SSO, Security (which is selected and highlighted in orange), Ftp Management, Reports, User Preferences, and Notifications. On the left, a sidebar menu under the "Users" heading lists Multi-Domain Users, Permission Sets (with an orange arrow pointing to it), Roles, Settings, Two Factor Authentication, and SFTP Management. The main content area is titled "Users" and shows a search bar with "ad car" and a "Search" button. There are checkboxes for "Include Inactive Users" and "Show Vendor Users" with a "Show All" link. A table displays a single user row: "Ad Car (ad.car.demo)". Below the table, a note says "*Indicates the Domain Administrator". To the right of the table, there are tabs for General (which is selected and highlighted in blue), Accounts, Permissions, Landing Page, Roles, Reset Password, and 2FA. A note below the tabs says "Fields marked with an asterisk(*) are required." and "Password History". The "General" tab contains several input fields:

- *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)

A large orange rectangle highlights the "First Name", "Last Name", "Email", "Default Account", "Pool Id", and "Active" fields. At the bottom right of the "General" tab is a blue "Save General Settings" button.

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 portal interface. The top navigation bar includes links for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT, and Payments. The ACCOUNT tab is selected. Below the navigation is a sub-menu with links for Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in red), Ftp Management, Reports, User Preferences, and Notifications. The main content area is titled 'Account' and has a sidebar on the left with links for Users, Multi-Domain Users, Permission Sets (with an orange arrow pointing here), Roles, Settings, Two Factor Authentication, and SFTP Management. The main panel is titled 'Users' and shows a search bar with 'ad car' and a 'Search' button. There are checkboxes for 'Include Inactive Users' and 'Show Vendor Users' with a 'Show All' link. A table lists a single user: 'Ad Car (ad.car.demo)'. The table has tabs for General, Accounts, Permissions, Landing Page, Roles, Reset Password, and 2FA. The 'General' tab is selected. The user details include: *User Name: ad.car.demo, *First Name: Ad, *Last Name: Car, *Email: ad.car@star.com, *Default Account: America Healthcare Inc (729), Pool Id: Waystar Portal Standard Login Users, and Active (checkbox). Below the table are checkboxes for Force user to change password and Clear users security questions. At the bottom right is a blue 'Save General Settings' button.

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 the Waystar User Management interface. The window title is "America Healthcare Inc (729)". Under "Pool Id:", "Waystar Portal Standard Login Users" is selected. The "Active" checkbox is checked. Below it are three other checkboxes: "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.)". The "Reactivate Account" checkbox is currently unchecked. At the bottom right is a blue "Save General Settings" button.

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

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

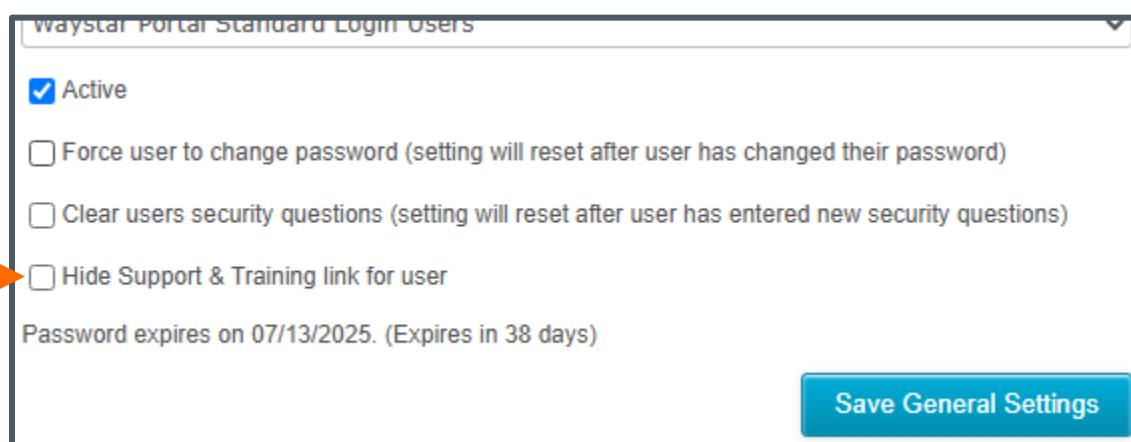
Hiding the Support and Training Center link

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.

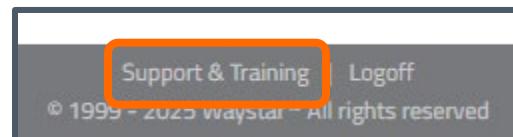
To hide the STC link:

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.

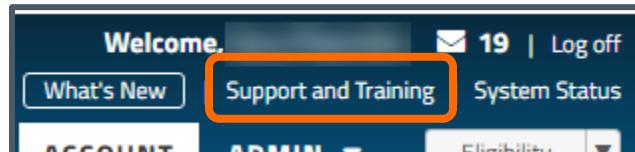


The selected user will no longer see the STC link in the Waystar portal, such as in the following locations:

- 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 'Users' section of the Waystar Health account management system. On the left, there's a sidebar with links for 'Multi-Domain Users', 'Permission Sets', 'Roles', 'Settings', and 'Two Factor Authentication'. The main area is titled 'Users' and shows a search bar with '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 table lists a single user: 'Ad Car (ad.car.demo)'. To the right of the table are tabs for 'General', 'Accounts', 'Permissions', 'Landing Page', 'Roles', 'Reset Password', and '2FA'. An orange arrow points to the 'History' link under the 'General' tab. Below the table, a note says '*Indicates the Domain Administrator'. At the bottom, it says 'Fields marked with an asterisk(*) are required.' and shows a user name field with 'ad.car.demo'. There's also a 'Password History' link.

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

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 screenshot shows the Waystar Health account management interface. The top navigation bar includes links for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT, and Payments. The ACCOUNT tab is active. Below the navigation, there are tabs for Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in red), Ftp Management, Reports, User Preferences, and Notifications. On the left, a sidebar menu has 'Users' selected, with options for Multi-Domain Users, Permission Sets, Roles, Settings, and Two Factor Authentication. The main content area displays a table titled 'Users' with a single row for 'Ad Car (ad.car.demo)'. The table includes columns for General, Accounts, Permissions, Landing Page, Roles, Reset Password, and 2FA. A note below the table states '*Indicates the Domain Administrator'. At the bottom of the table, it says 'Fields marked with an asterisk(*) are required.' and shows a user name 'ad.car.demo'. An orange arrow points from the 'Password History' link in the top right corner of the page to the 'History' link in the bottom right corner of the user table.

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

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 User Management interface. On the left, there's a sidebar with 'Users' selected, followed by 'Multi-Domain Users', 'Permission Sets', 'Roles', 'Settings', 'Two Factor Authentication', and 'SFTP Management'. The main area is titled 'Users' and shows a list of users: 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), and Am Clar (am.clar.demo). Above the user list is a search bar with 'User Name' and 'Search' buttons, and checkboxes for 'Include Inactive Users' and 'Show Vendor Users' with a 'Show All' link. Below the user list are buttons for 'New User', 'Accounts' (which is highlighted with an orange arrow), 'Permissions', 'Landing Page', 'Roles', 'Reset Password', and '2FA'. At the bottom of the list, there are checkboxes for 'Check All' and 'Include Hidden Accounts'. To the right of the user list, there's a column of 'Account History' with 'Report' links next to each account name. An orange arrow points to the 'Accounts' tab, another points to the 'Check All' checkbox, and a third points to the 'Include Hidden Accounts' checkbox.

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 Waystar portal interface. At the top, there is a navigation bar with links: MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT, and Payments. The ACCOUNT link is highlighted. Below the navigation bar, the page title is "Account". Under the "Account" title, there are several tabs: Summary, Enrollment, Account Profile, SSO, Security (which is underlined in red), Ftp Management, Reports, User Preferences, and Notifications. The "Security" tab is currently active. On the left side, there is a sidebar with the following menu items: Users (which is also underlined in red), Multi-Domain Users, Permission Sets (with an orange arrow pointing to it), Roles, Settings, Two Factor Authentication, and SFTP Management. The main content area is titled "Users" and shows a search bar with "ad car" and a "Search" button. There is a checkbox for "Include Inactive Users" and another for "Show Vendor Users", both of which are unchecked. A "Show All" link is also present. Below the search bar, a user named "Ad Car (ad.car.demo)" is listed. To the right of the user name, there are several buttons: General, Accounts, Permissions (with an orange arrow pointing to it), Landing Page (which is underlined in blue), Roles, Reset Password, and 2FA. Below these buttons, a note says "*Indicates the Domain Administrator". Further down, there is a section titled "Choose a new homepage from the list below or paste a custom Waystar URL". This section contains two dropdown menus: "Site Section" (set to "Analytics") and "Page" (set to "Work Spaces"). To the right of these dropdowns, there is an "OR" option and a "Custom URL" field containing the URL "https://dataexplorer.zirmed.com/Workspa". At the bottom right of the page, there is a blue "Save Landing Page" button.

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.

Note: The URL you provide must be from a screen the user can access while logged into Waystar.

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 Health software interface. At the top, there is a navigation bar with links: MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT, ADMIN, and Payments. The ADMIN link is currently selected. Below the navigation bar, the page title is "Account". Under the "Account" title, there are several tabs: Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in red), Reports, User Preferences, Account Breakout, and Notifications. On the left side, there is a sidebar with the following menu items: Users, Multi-Domain Users, Permission Sets (with an orange arrow pointing to it), Roles (which is highlighted in orange), Settings, Two Factor Authentication, and SFTP Management. The main content area is titled "Roles". It contains a search bar with fields for "Role Name" and "Search", and a "Show All" button. Below the search bar, there is a table with columns: General, Accounts, and Permissions (with an orange arrow pointing to it). The table lists various roles: AMD Role, CBO Biller, Front Desk, PNC, Provider Implementations, and Security Manager. At the bottom of the table, there is a page navigation bar showing "Page 1 of 1". To the right of the table, there is a list of users, each with a checkbox next to their name. Some checkboxes are checked (e.g., Ad Fum, Al Val, Al Cher) while others are not (e.g., Ad Car, Ad Young, Al Hu, Al Ware). A red box highlights this 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 shows the Waystar Health software interface. The top navigation bar includes links for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT (which is highlighted), and Payments. The main content area is titled 'Account' and contains a 'Users' section. On the left, there is a sidebar with links for Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in red), Ftp Management, Reports, User Preferences, and Notifications. The 'Users' section has a search bar with 'ad car' and a 'Search' button. It also includes filters for 'Include Inactive Users' and 'Show Vendor Users' with a 'Show All' link. Below the search bar, a user named 'Ad Car (ad.car.demo)' is listed, with a note indicating they are the 'Domain Administrator'. There are tabs for General, Accounts, Permissions, Landing Page, Roles (which is highlighted in blue), Reset Password, and 2FA. Under the Roles tab, a list of roles is shown with checkboxes: 'CBO Biller' (unchecked), 'Front Desk' (checked), 'PNC' (unchecked), 'Provider Implementations' (unchecked), and 'Security Manager' (unchecked). An orange arrow points to the 'Permission Sets' link in the sidebar, another points to the 'Roles' tab in the top bar, and a third points to the 'Front Desk' checkbox in the list.

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 portal interface. At the top, there is a navigation bar with tabs: MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, ACCOUNT, and Payments. The ACCOUNT tab is active. Below the navigation bar, the page title is "Account". Under the "Account" title, there is a sub-navigation menu with tabs: Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in red), Ftp Management, Reports, User Preferences, and Notifications. On the left side, there is a sidebar with a vertical list of options: Users (which is also highlighted in red), Multi-Domain Users, Permission Sets, Roles, Settings, Two Factor Authentication, and SFTP Management. The main content area is titled "Users". It displays a search bar with the text "ad car" and a "Search" button. There are two checkboxes: "Include Inactive Users" and "Show Vendor Users", followed by a "Show All" link. A user entry "Ad Car (ad.car.demo)" is listed, with a note below it stating "*Indicates the Domain Administrator". To the right of the user entry are several tabs: General, Accounts, Permissions, Landing Page, Roles, Reset Password (which is highlighted in blue), and 2FA. Below these tabs, there are two radio buttons: "Set password expiration to tomorrow" (unchecked) and "Set new password" (checked). Below the radio buttons are fields for "New Password" and "Confirm Password", both of which are currently empty. At the bottom right of the form is a blue "Save Password" button.

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 Waystar User Management interface. At the top, there's a search bar with '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 table lists a single user: 'Ad Car (ad.car.demo)' with a status of 'Active'. Below the table are navigation buttons for 'Page 1 of 1'. To the right of the user list is a horizontal navigation bar with tabs: General, Accounts, Permissions, Landing Page, Roles, Reset Password, and 2FA. The '2FA' tab is highlighted with an orange arrow pointing to it. Below the navigation bar, a note says '*Indicates the Domain Administrator'. Under the '2FA' tab, a section titled 'Two Factor Authentication' contains the message: 'Two Factor Authentication (2FA) has not been enabled. This section will remain inactive until 2FA has been turned on.' An orange arrow points to the 'Enable 2FA' link below this message.

- 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

User Name	Search	<input checked="" type="checkbox"/> Include Inactive Users	<input type="checkbox"/> Show Vendor Users	Show All
<input type="button" value="General"/> <input type="button" value="Accounts"/> <input type="button" value="Permissions"/> <input type="button" value="Landing Page"/> <input type="button" value="Roles"/> <input type="button" value="Reset Password"/> <input type="button" value="2FA"/>				
Two Factor Authentication <p>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.</p>				
<input type="button" value="Generate code for this user"/> <input type="button" value="Send code to user"/>				
Temporary Code: 345127				

*Indicates the Domain Administrator

- **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

User Name	Search	<input checked="" type="checkbox"/> Include Inactive Users	<input type="checkbox"/> Show Vendor Users	Show All
<input type="button" value="General"/> <input type="button" value="Accounts"/> <input type="button" value="Permissions"/> <input type="button" value="Landing Page"/> <input type="button" value="Roles"/> <input type="button" value="Reset Password"/> <input type="button" value="2FA"/>				
Two Factor Authentication <p>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.</p>				
<input type="button" value="Generate code for this user"/> <input type="button" value="Send code to user"/>				
Select a method from below: <p><input type="radio"/> Email on File *****maluser@test.com</p> <p><input type="radio"/> Manual Entry <input type="button" value="Text"/></p> <p>Phone Number <input type="text" value="_____ - _____ - _____"/></p> <input type="button" value="Send Code"/>				

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.

The screenshot shows the 'Account' section of the Waystar Health interface. The top navigation bar includes 'MY WORK', 'CLAIMS PROCESSING', 'PATIENT TOOLS', 'ANALYTICS', 'MEDICARE', and 'ACCOUNT'. Below this, a secondary navigation bar has tabs for 'Summary', 'Enrollment', 'Account Profile', 'SSO', 'Security' (which is highlighted in red), 'Reports', 'User Preferences', 'Account Breakout', and 'Notifications'. On the left, a sidebar menu lists 'Users', 'Multi-Domain Users', 'Permission Sets', 'Roles', 'Settings' (which is also highlighted in red), 'Two Factor Authentication', and 'SFTP Management'. The main content area is titled 'Settings' and contains two main sections: 'Automatically deactivate any user who hasn't logged in in [3] months.' and 'Users must reset passwords every [60] days.' A checkbox for 'Restrict Login by IP Address' is present but unselected. Below this is a section for managing IP addresses, showing 'Current IP Address: 10.15.31.246' and buttons for 'Add' and 'Remove Selected IP Address'. At the bottom right is a large 'Save Security Settings' button.

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.

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

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

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' section of the Waystar Health interface. The top navigation bar includes links for MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is selected. Below the navigation is a sub-menu with links for Summary, Enrollment, Account Profile, SSO, Security (which is highlighted in red), Reports, User Preferences, Account Breakout, and Notifications. The main content area is titled 'Settings'. It contains several configuration options: 'Automatically deactivate any user who hasn't logged in in [3] months.', 'Users must reset passwords every [60] days', and a checkbox for 'Restrict Login by IP Address' which is currently unchecked. A list of 'Accepted IP Addresses' is shown, with one entry '10.15.31.246' listed. To the right of this list are 'Add' and 'Remove Selected IP Address' buttons. An orange arrow points to the 'Remove Selected IP Address' button. At the bottom right of the settings area is a large orange arrow pointing to the 'Save Security Settings' button. The left sidebar has a vertical list of links: Users, Multi-Domain Users, Permission Sets, Roles, Settings (which is highlighted in orange), Two Factor Authentication, and SFTP Management.

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**.

The screenshot shows the Waystar Account interface. At the top, there's a blue header bar with the word 'ACCOUNT' in white. Below it, a secondary navigation bar has tabs: 'Account Profile', 'SSO', 'Security' (which is highlighted in orange), 'Ftp Management', 'Reports', 'User Preferences', and 'Notifications'. On the left side, there's a vertical sidebar with links: 'Users', 'Multi-Domain Users', 'Permission Sets' (which is also highlighted in orange), 'Roles', 'Settings', 'Two Factor Authentication', and 'SFTP Management'. The main content area is titled 'Permission Sets'. It features a search bar with fields for 'Permission Name' and 'Search', and a 'Show All' button. Below the search bar, there's a button labeled '+ New Permission Set'. Underneath, two permission sets are listed: 'All Non-Administrative Permissions' and 'Manage Users - All Security Functions'. At the bottom of this list, there's a pagination control showing 'Page 1 of 1'.

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.

ACCOUNT

Account

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

Users

Multi-Domain Users

Permission Sets

All Non-Administrative Permissions

Manage Users - All Security Functions

Page 1 of 1

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

General Member Of

Fields marked with an asterisk(*) are required.

*Name:
AllAuthProducts

*Description:
Permission set for access to all legacy recondo auth products

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

The screenshot shows the 'Permission Sets' screen with the 'Member Of' tab selected. A list of permission sets is on the left, and the 'Auth Status - General' checkbox is selected under the 'Auth Status (1)' section. An orange arrow points to this checkbox.

Permission Set	Description	Type
All Non-Administrative Permissions	Any user who has the permission AllAuthProducts will also get the permissions checked below.	
AllAuthProducts		
AuthInitiateOnly		
Manage Users - All Security Functions		
WaystarApplications		
<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		

7. 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:

1. Go to **ACCOUNT > Security > Permission Sets**.
- The Permission Sets screen will open.
2. Locate the permission set name you want to edit. You can use the search field at the top of the screen.
 3. From the list of permission set names, click the one you want to edit.
 4. Click the **Member Of** tab.
 5. Select or clear (unselect) the checkboxes of the appropriate permissions.
 6. 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:

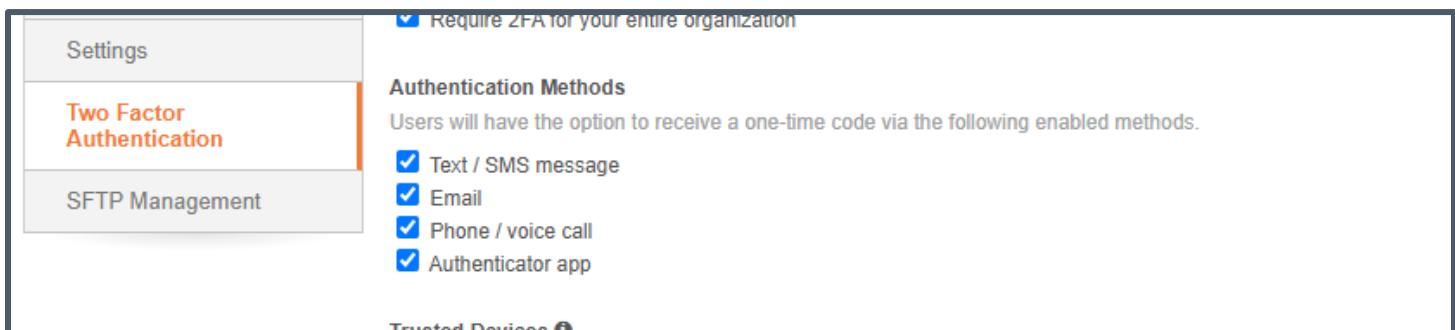
1. Go to **ACCOUNT > Security > Two Factor Authentication.**

The Two Factor Authentication screen will open.

The screenshot shows the Waystar portal interface with the 'ACCOUNT' tab selected. On the left, a sidebar menu lists 'Users', 'Multi-Domain Users', 'Permission Sets', 'Roles', 'Settings', 'Two Factor Authentication' (which is highlighted in red), and 'SFTP Management'. The main content area is titled 'Two Factor Authentication'. It contains a descriptive paragraph about 2FA, a note about SSO, and several configuration sections: 'Require 2FA' (with a checked checkbox), 'Authentication Methods' (checkboxes for 'Text / SMS message', 'Email', 'Phone / voice call', and 'Authenticator app'), 'Trusted Devices' (radio buttons for 'Trusted devices off' and 'Trusted devices on' - the latter is selected), and a dropdown menu for 'Users must provide 2FA at login every' (options are 30 Days, 1 Day, 7 Days, and 30 Days, with 7 Days currently selected). A small orange arrow points to the '7 Days' option in the dropdown.

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.



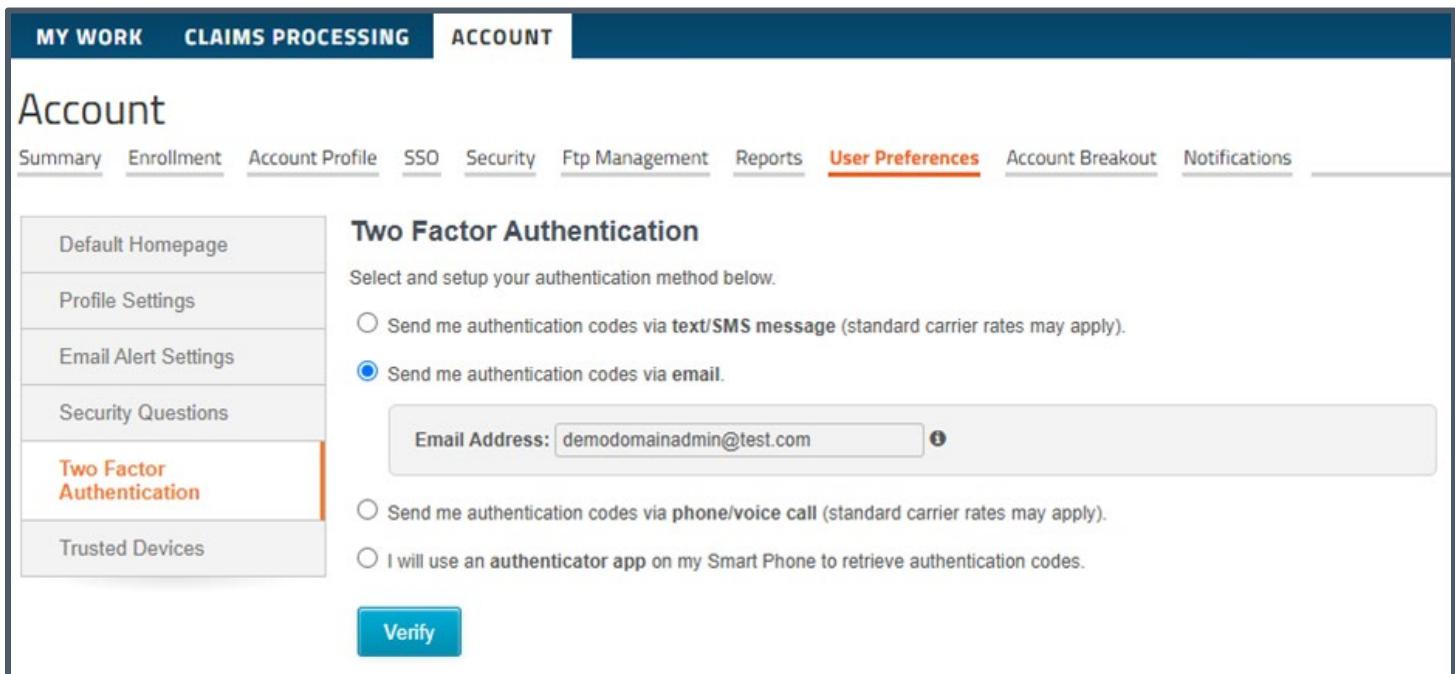
Require 2FA for your entire organization

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

- 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

Default Homepage
Profile Settings
Email Alert Settings
Security Questions
Two Factor Authentication
Trusted Devices

Two Factor Authentication

Select and setup your authentication method below.

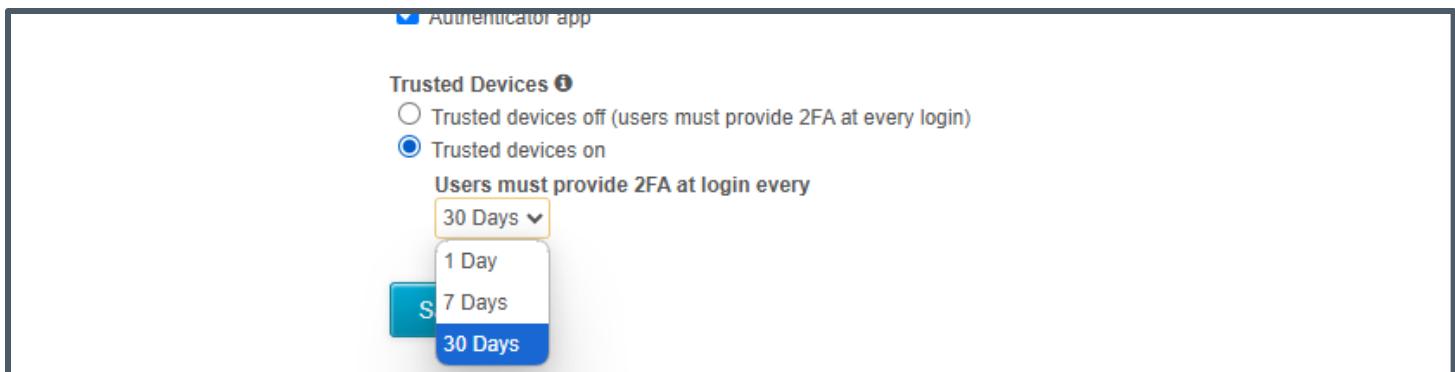
Send me authentication codes via text/SMS message (standard carrier rates may apply).
 Send me authentication codes via email.

Email Address: demodomainadmin@test.com

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.



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.

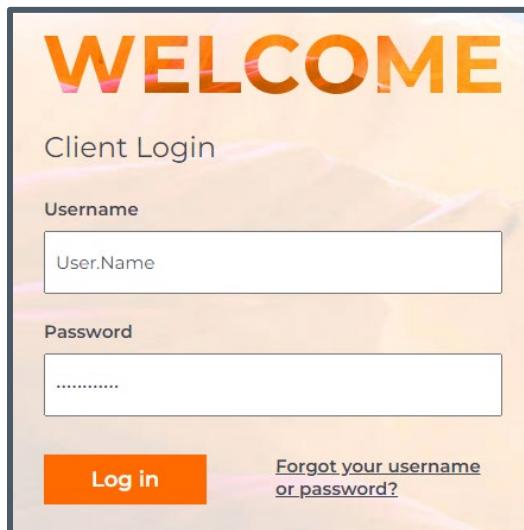
Using two-factor authentication

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.

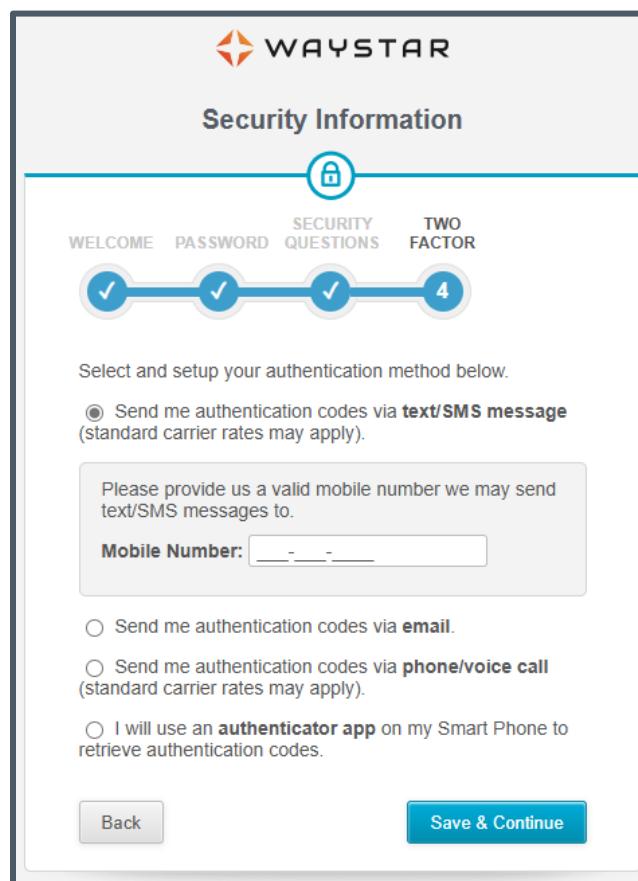
To use two-factor authentication:

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



The screenshot shows the Waystar Client Login page. At the top is a large orange 'WELCOME' banner. Below it is the text 'Client Login'. There are two input fields: 'Username' (containing 'User.Name') and 'Password' (containing '.....'). Below these is an orange 'Log in' button and a blue link 'Forgot your username or password?'

The initial Two Factor Authentication screen will open.



The screenshot shows the 'Security Information' step of the two-factor setup. At the top is the Waystar logo and the title 'Security Information'. Below is a horizontal progress bar with four circles: 'WELCOME' (checked), 'PASSWORD' (checked), 'QUESTIONS' (checked), and 'TWO FACTOR' (step 4). A teal lock icon is above the progress bar. Below the progress bar is the text 'Select and setup your authentication method below.' There are four radio button options:

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

A text input field for 'Mobile Number' is shown with the placeholder 'Please provide us a valid mobile number we may send text/SMS messages to.' At the bottom are 'Back' and 'Save & Continue' buttons.

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

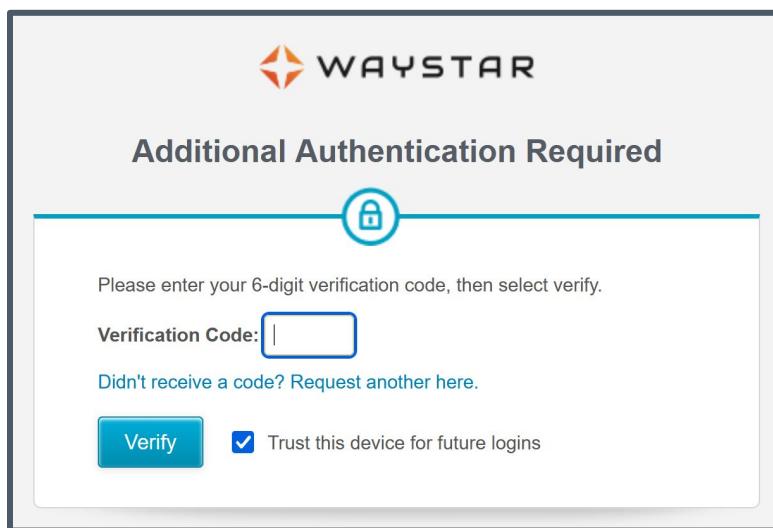
- Text/SMS message
- Email
- Phone/Voice Call
- Authenticator App

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.



The image shows a screenshot of a web page titled "Additional Authentication Required". At the top center is the Waystar logo. Below it, the title "Additional Authentication Required" is displayed in bold. In the center, there is a blue circular icon containing a white padlock symbol. Below the icon, a message reads "Please enter your 6-digit verification code, then select verify." To the left of this message is the label "Verification Code:" followed by an empty input field. To the right of the input field is a small placeholder character "|". Below the input field is a link in blue text that says "Didn't receive a code? Request another here.". At the bottom left is a blue rectangular button labeled "Verify". To the right of the "Verify" button is a checkbox with a checked mark and the text "Trust this device for future logins".

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).

The screenshot shows the Waystar Health application interface. At the top, there is a navigation bar with tabs: MY WORK, CLAIMS PROCESSING, PATIENT TOOLS, ANALYTICS, MEDICARE, and ACCOUNT. The ACCOUNT tab is currently selected. Below the navigation bar, the page title is "Account". Under the account title, there is a sub-navigation menu with links: Summary, Enrollment, Account Profile, SSO, Security, Reports (which is highlighted in red), User Preferences, Account Breakout, and Notifications. The main content area is titled "System Access Report" and includes a "By User" dropdown set to "All". Below this, there is a "Date Range" section with several filter options. On the left, there are radio buttons for selecting a time period: This Month, Last Month, This Quarter, Last Quarter, This Year, and Custom. The "This Month" option is selected. Next to these are input fields for "From" (9/1/2023) and "To" (9/30/2023). On the right, there are two radio buttons: "Active Users" (selected) and "InActive Users". Below these is a dropdown menu with "All" selected. At the bottom of the "Date Range" section is a "Generate Report" button.

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” sectionUpdated the “Enabling (requiring) two-factor authentication” section	6
February 2025	Reviewed and updated the guide throughout	5