System Administration

System Administration

Version : 22.01

Published : May 2025

TruBridge
54 St. Emanuel Street
Mobile, AL 36602
T(877) 424-1777
trubridge.com

Table of Contents

Chapter 16 Logging into Web Client

Chapter 17 Forgot Password via Web Client

Chapter 1 Introduction

1.1 Attestation Disclaimer

Promoting Interoperability Program attestation confirms the use of a certified Electronic Health Record (EHR) to regulatory standards over a specified period of time. TruBridge Promoting Interoperability Program certified products, recommended processes and supporting documentation are based on TruBridge's interpretation of the Promoting Interoperability Program regulations, technical specifications and vendor specifications provided by CMS, ONC and NIST. Each client is solely responsible for its attestation being a complete and accurate reflection of its EHR use during the attestation period and that any records needed to defend the attestation in an audit are maintained. With the exception of vendor documentation that may be required in support of a client's attestation, TruBridge bears no responsibility for attestation information submitted by the client.

1.2 What's New

This section introduces the new features and improvements to **System Administration** for release Version 22.01. A brief summary of each enhancement is given referencing its particular location if applicable. As new branches of Version 22.01 are made available, the original enhancements will be moved to the Previous Work Requests section. The enhancements related to the most current branch available will be listed under the main What's New section.

Each enhancement includes the Work Request (WR) Number and the description. If further information is needed, please contact **Client Services** Support.

Credentials Effective Date Added to Employee Setup -- FA-12373

DESCRIPTION: A Credentials Effective Date field has been added to the Employee Setup and Maintenance screen. This field allows the date the credentials became effective for the employee to be entered. This ensures that if a user's credentials were to change, the credentials are updated accordingly on any new edits or addendums to notes that were previously signed with the original credentials.

The history of all changes made will be displayed within Payroll on the Changes to Employee Master screen.

DOCUMENTATION: See Employee Setup and Maintenance 7

Forgot Password via Web Client -- EVI-123792

DESCRIPTION: The 'Forgot Password' feature allows users to reset their TruBridge EHR password directly from the Web Client login screen, without the need for administrator assistance.

DOCUMENTATION: See Forgot Password via Web Client 147

Patient Data Console - New Behavior Control -- FA-11988

DESCRIPTION: A new behavior control titled 'Patient Chart - Verify and Unverifiable Actions' has been created for the Patient Data Console application. This behavior control designates which users have permission to perform the Verify/Unverifiable workflow.

The following roles will have this behavior control set to Active by default:
- Physician Group
- Registered Nurse
- Licensed Practical Nurse

DOCUMENTATION: See Patient Data Console 125

Chapter 2 Overview

The System Administration module is a central location where all users are set up in the system with a user login to give them access to the facility. Once a user login has been created, security will need to be given. This user guide will address the processes of how to set up a user login, how to login with the new user login and how to give access within the facility.

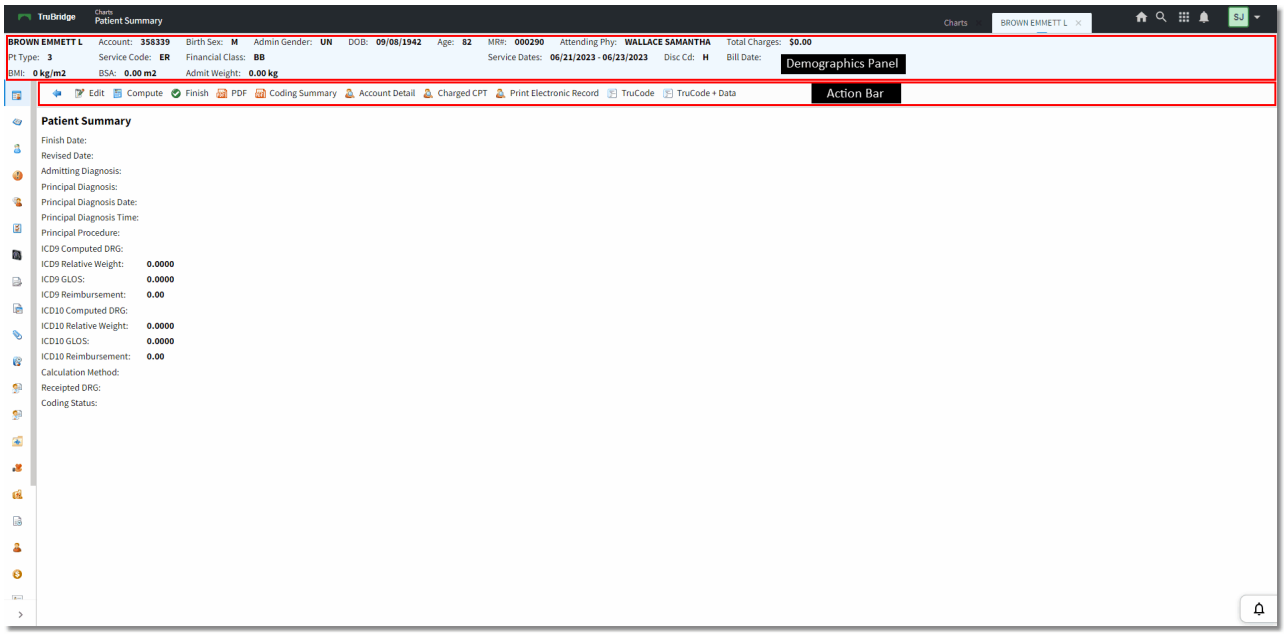
NOTE: *Facilities outside of the United States may choose a date format of MMDDYY, DDMMYY or YYMMDD to be used on all date fields in the System Administration Application. Where four-digit dates display, a date format of MMDD, DDMM or MMDD, respectively, will be used. Whichever date format is selected will be reflected in all date fields and column displays throughout the application. A TruBridge Representative should be contacted in order for the date format to be changed.*

Chapter 3 System Administration

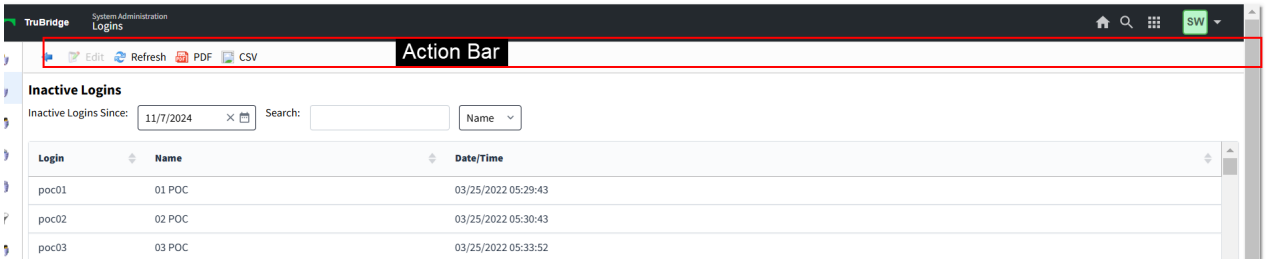
The System Administration application is where user logins are created and security rules are assigned to determine what a user will have access to within TruBridge EHR. Keep in mind, user security is currently maintained in two locations. Security for traditional screens and reports (CW4) will still be maintained via System Security in the System Management application (Path: Web Client > System Menu > Special Functions > System Management > System Security > Employee Security/Physician Security). While security for updated screens and reports (CW5) will be maintained via security rules in System Administration. Security must be addressed in both locations for each user. For more information on System Security please see the System Management User Guide.

CW5 Screens

CW5 screens are typically screens that are **NOT** accessed from the System Menu. However, some applications within the System Menu have begun to be converted to use some CW5 screens. One way to identify a CW5 vs. CW4 screens when using the System Menu applications is to look at the top of the screen for the presence of a Demographics Panel (if on a patient's account) or an Action Bar. These two features are typically present on CW5 screens. Below you will see an example of these features.



CW5 Demographics Panel and Action Bar - From Patient Account



CW5 Action Bar - Not on Patient Account

CW5 Reports

CW5 reports are those reports that were programmed using Report Writer Templates. These reports are available on the Report Dashboard. Keep in mind, some existing reports have been updated from their original format and when accessed from their traditional paths (within the System Menu), will launch the Report Writer version.

System Administration Security

System Administration is where user logins are created and where security rules are assigned to control user access to CW5 screens and reports. System Administration login security begins by assigning the login to a role. The role identifies the users function within the organization and may have a set of security rules attached to it. TruBridge default roles are available to choose from; however, custom roles may be created as well. Security rules may be assigned to roles. Rules assigned to a role will affect all logins that are assigned to that role. Rules may also be added to individual logins.

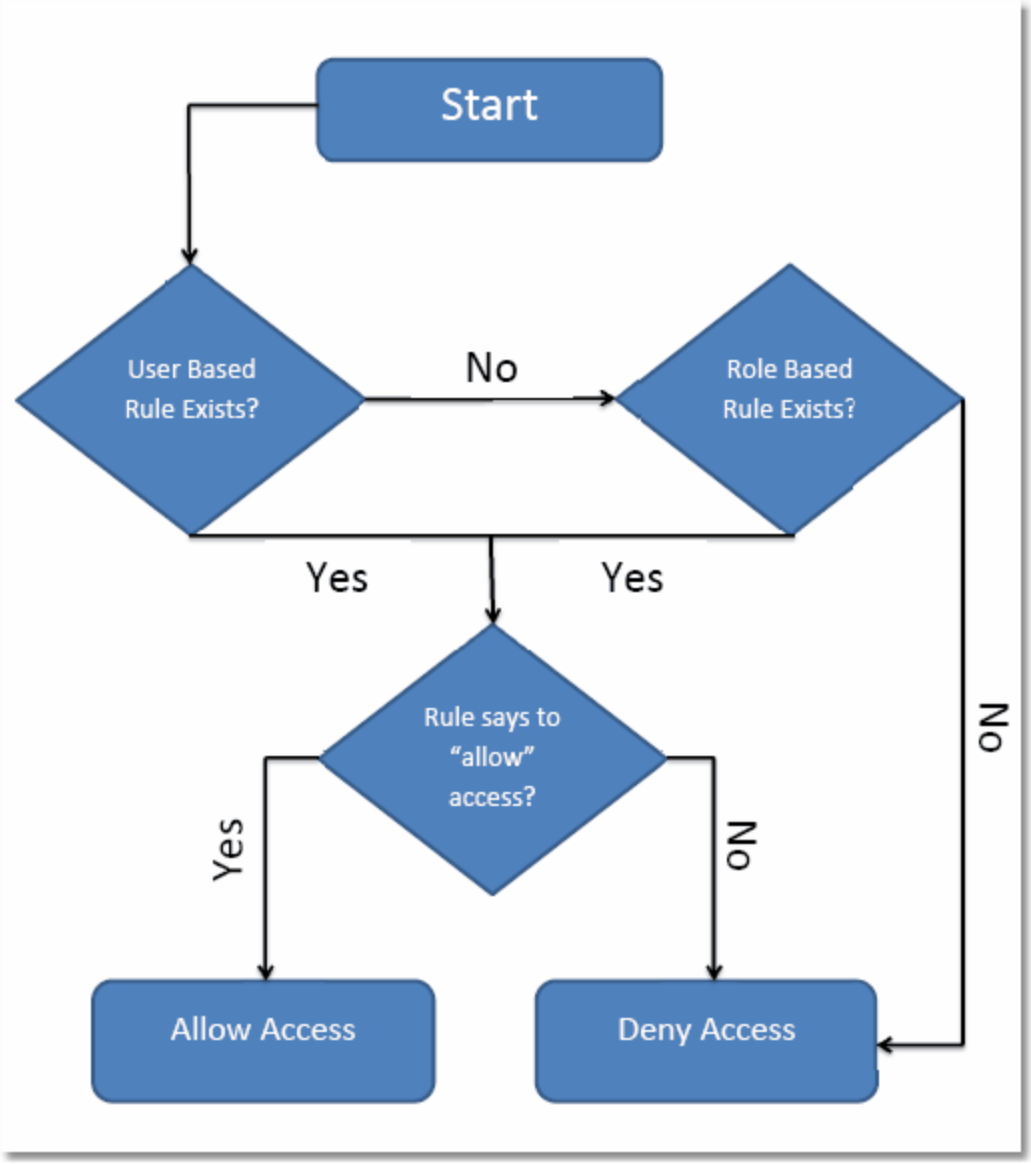
Different types of security rules exist to determine what access a user should have in an area of the system. These include Application, Screen, Report and Behavior Control rules.

- **Application**: Each screen and report is tied to an application. Using an application security rule will control access to all CW5 screens and all Report Writer reports that belong to an application.
- **Screen**: Controls access to specific CW5 screens within an application.
- **Report**: Controls access to specific Report Writer reports within an application.
- **Behavior Control**: Determines what actions a user may take when using a specific CW5 screen or Report Writer report. Keep in mind that not all actions require a behavior control. A list of behavior controls and their use may be found in the Behavior Control Definitions 110 section of this user guide.

A rule must both exist and be allowed in order for access to be granted. If there is an explicit deny or an absence of a rule, the system will deny the user.

The security on the login will always take precedence over the security assigned to a role. For example: A user is placed in the Scheduler's role. The role has security to the following applications: Report Writer, Home Screen and Electronic Signature. However, the user also needs to be able to access the Temp Registration screen through ChartLink. Because the Scheduler's role does not have access to ChartLink, the individual user may be granted access to the Temp Registration screen.

The following is a flowchart to demonstrate how rule precedence works.

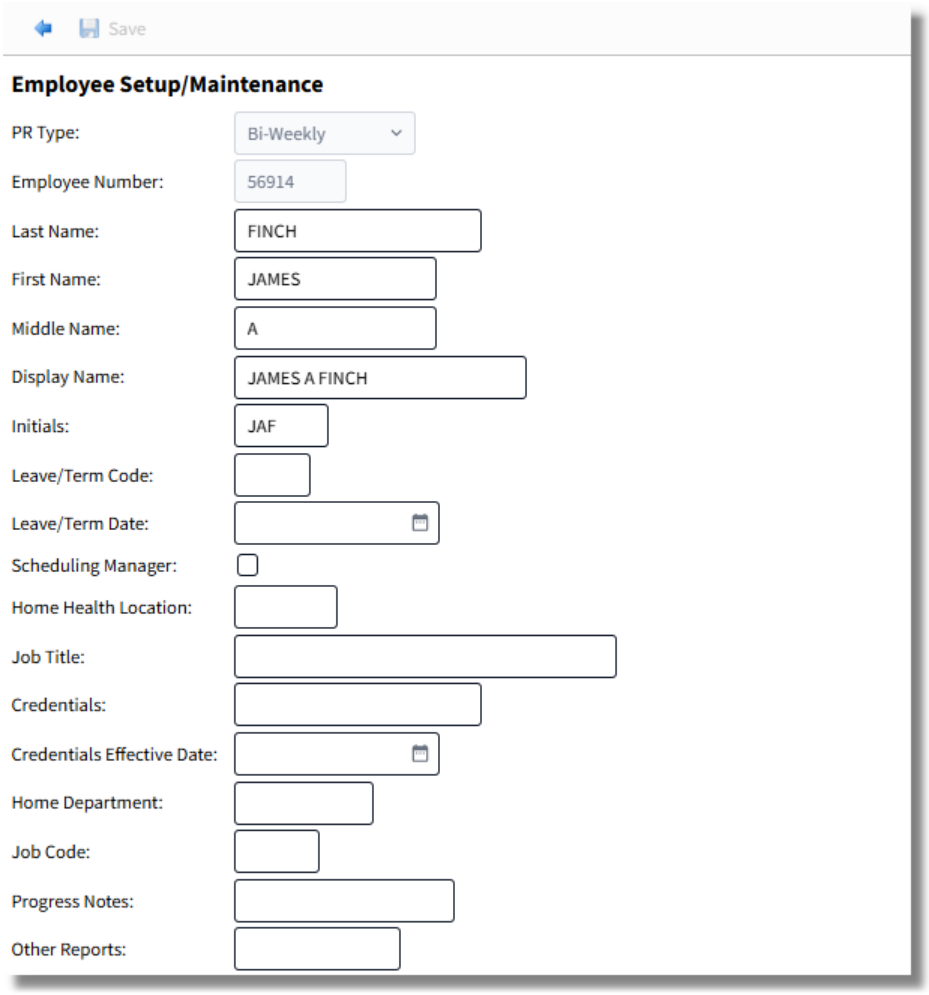


Rule Based Security Precedence Flowchart

Chapter 4 Employee Setup and Maintenance

The Employee Setup and Maintenance screen allows for the creation of a non-provider employee number.

Select **Web Client** > **System Administration** > **Employee Setup/Maintenance** > **New**



Employee Setup/Maintenance

- **PR Type**: Select the appropriate payroll type of Bi-Weekly, Monthly, Semi-Monthly or Weekly.
- **Employee Number**: Will automatically populate with the next available Employee Number. An employee number may also be keyed in this field.
- **Last Name**: Enter the employee's last name.

NOTE: *No punctuation should be used when completing the employee name fields.*

- **First Name**: Enter the employee's first name.

- **Middle Name**: Enter the employee's middle name or middle initial.
- **Display Name**: The employee's first name, middle initial and last name will appear in this field once the first three fields have been completed.
- **Initials**:The employee's initials will appear in this field once the first three fields have been completed.
- **Leave/Term Code**: The leave termination code is a one-character, facility-defined field used to indicate if the employee is on leave or if the employee has been terminated by the facility.
- **Leave/Term Date**: Select the date the employee left the job in this field.
- **Scheduling Manager**: Select this option to allow the employee to schedule visits for other home health employees.
- **Home Health Location**: Enter the employee's Home Health Location code.
- **Job Title**: Enter the employee's job title.
- **Credentials**: The employee's Credentials may be entered in this field.
- **Credentials Effective Date**: This field indicates the date the user's credentials became active. It ensures the correct credentials are displayed when documentation is signed or addended, if the user's credentials are changed later.

NOTE: *Any changes made to this field will be displayed in Payroll on the Changes to Employee Master screen.*

- **Home Department**: Enter the employee's home department.
- **Job Code**:This field is used to store the two-character job classification code for this employee's normal job.
- **Progress Notes**:The Progress Notes field is a free-form field. When printing or reviewing Patient Progress Notes, the system will display exactly what is entered into this field in the Name field of the report. This field is only used for Point of Care Credentialing. It will consist of the first initial of the first name, last name and the credentials.
- **Other Reports**: The Other Reports field is a free form field. When printing or reviewing any Chart Cart report, other than Patient Progress Notes, the system will display exactly what is entered in this field. The information to be loaded is the employee's initials, followed by their credentials.

Employee Setup/Maintenance

Specialized Training Additions

- **Description**: Enter the description of the specialized license.
- **License #**: Enter the professional license number.
- **Expires**: Enter the date the license expires.

Select **Save** once all information has been captured.

***NOTE**: To access this screen, users must have access to the the following screens: **Employee Setup and Maintenance** and **Employee Setup and Maintenance List**.*

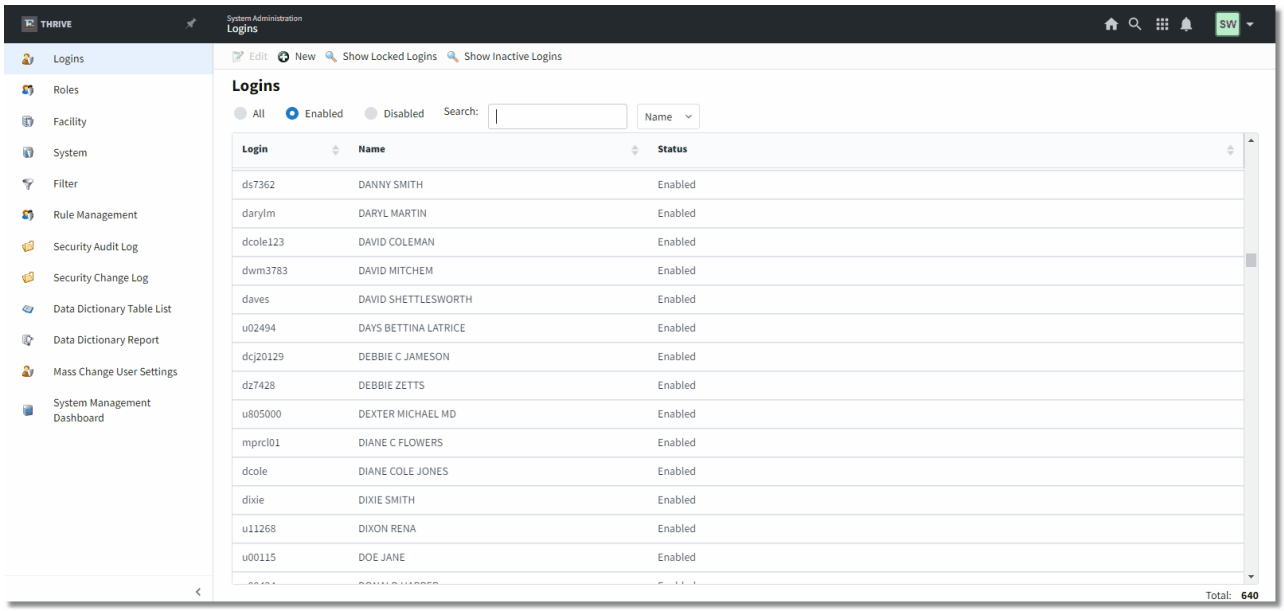
Chapter 5 Logins

After selecting System Administration, a listing of all enabled user logins will display. Radio buttons are also available to search for **Enabled**, **Disabled** or **All** user logins. The default will be **Enabled**.

A Smart Search tool is available throughout System Administration. This tool will be located at the top of the screen. To use the Smart Search tool, enter the search criteria in the Search field and select the preferred search method. The search is not case sensitive and will automatically find the string as it is entered.

The search option on the Logins screen may be used to find the login or name of an employee or physician.

Select **Web Client** > **System Administration**



System Administration

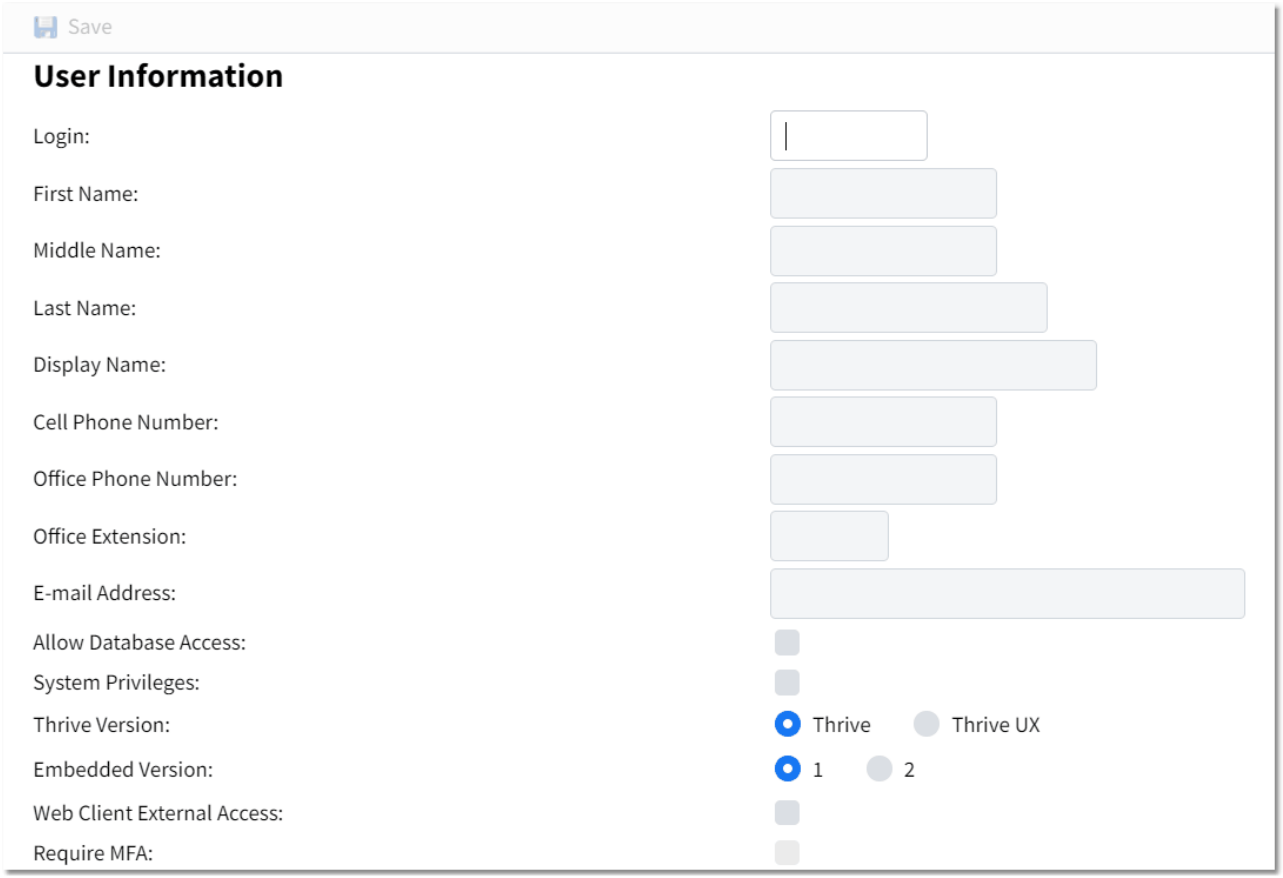
From the Logins screen new logins may be created and edited. Once a login is selected, security rules may be added to that login. When setting up security rules for a login, keep in mind that login rules supersede rules setup on the user's role.

NOTE: *In order to set up security rules for a login, the user adding the security must be in the System Administrator role.*

New Logins

To create a new user login, select **New** from the action bar on the Logins screen, and a blank User Information screen will display.

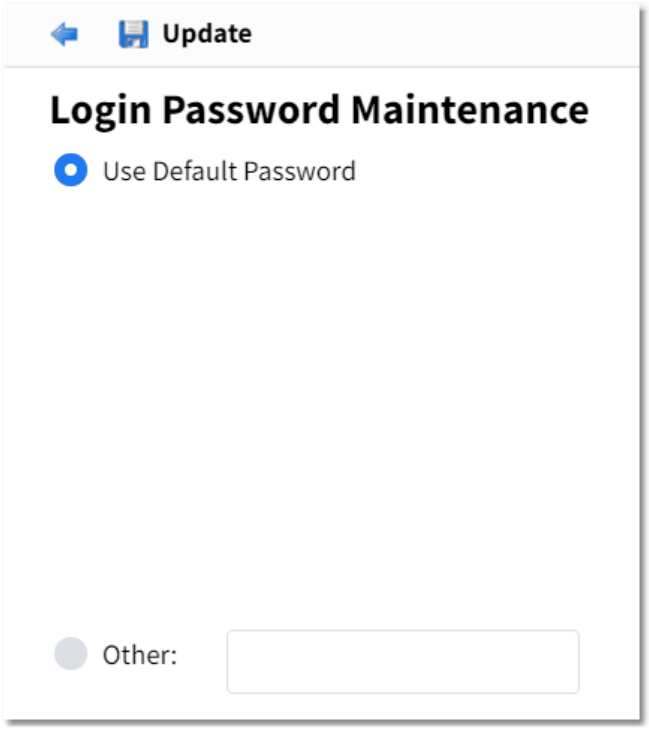
Select **Web Client** > **System Administration** > **Logins** > **New**



System Administration - Create a new Login

Please see the Maintenance 16 section for details on each field. After completing the User Information screen, select **Save** to continue setting up the new login. The Login Password Maintenance screen will then display.

Select **Web Client** > **System Administration** > **Logins** > **New** > **Save**



System Administration - Login Password Maintenance

This will determine the password that is used the first time the login accesses TruBridge EHR. After entering the password defined here, TruBridge EHR will allow a new password to be set up for the login. Two password options are available, select the radio button next to the appropriate option for the logname.

- **Use Default Password**: The logname will use TruBridge EHR's Default Password that is defined in the Login Policy located on the System screen in System Administration.
- **Other**: Enter a one-time password that the logname will use.

Select **Update** after completing the Login Password Maintenance screen.

For every login created, the default password is hashed using an SHA512 algorithm by TruBridge EHR Server OS. The resulting hash is then safely stored and used to compare the resulting hash of the user's "keyed" in password.

***NOTE**: In addition to creating the new login, the Facility 21 information as well as any additional security requirements (Application 32, Screen 43, Report 47, or Behavior Controls 39 Rules) will need to be address before the login is fully functional.*

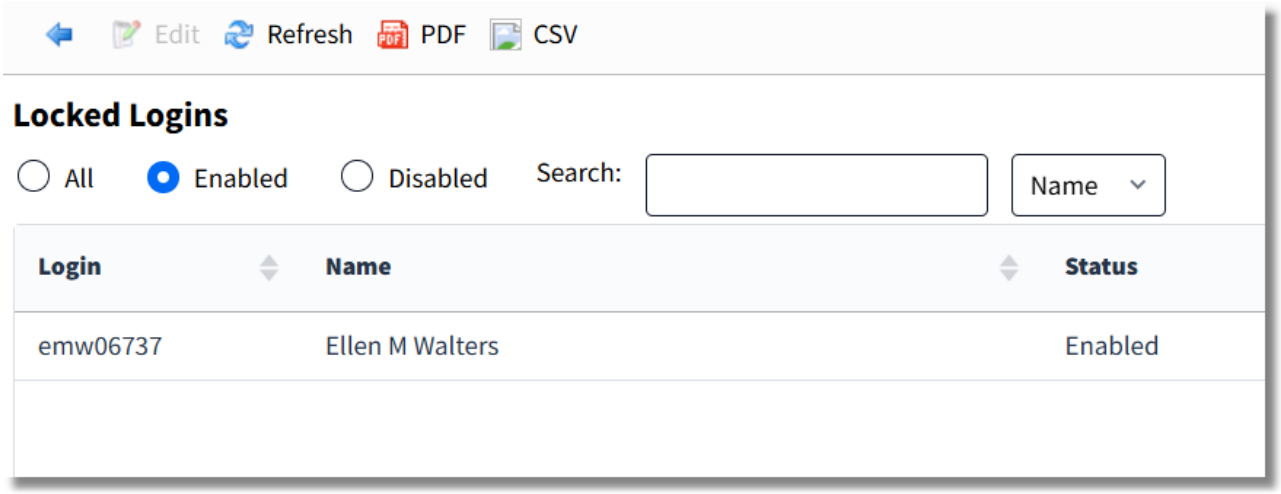
Show Locked Logins

The Show Locked Logins option will display all user logins that have been locked either due to the login being manually locked or having too many login attempts. To view the locked logins, select **Show Locked Logins** from the action bar on the Logins screen.

NOTE: *This option may take a while to run because the system will search through all logins to determine which ones are locked.*

Once Show Locked Logins is finished processing, the Locked Logins screen will display. The screen will display the user login, the name associated with the login and whether the login is enabled or disabled.

Select **Web Client** > **System Administration** > **Logins** > **Show Locked Logins**

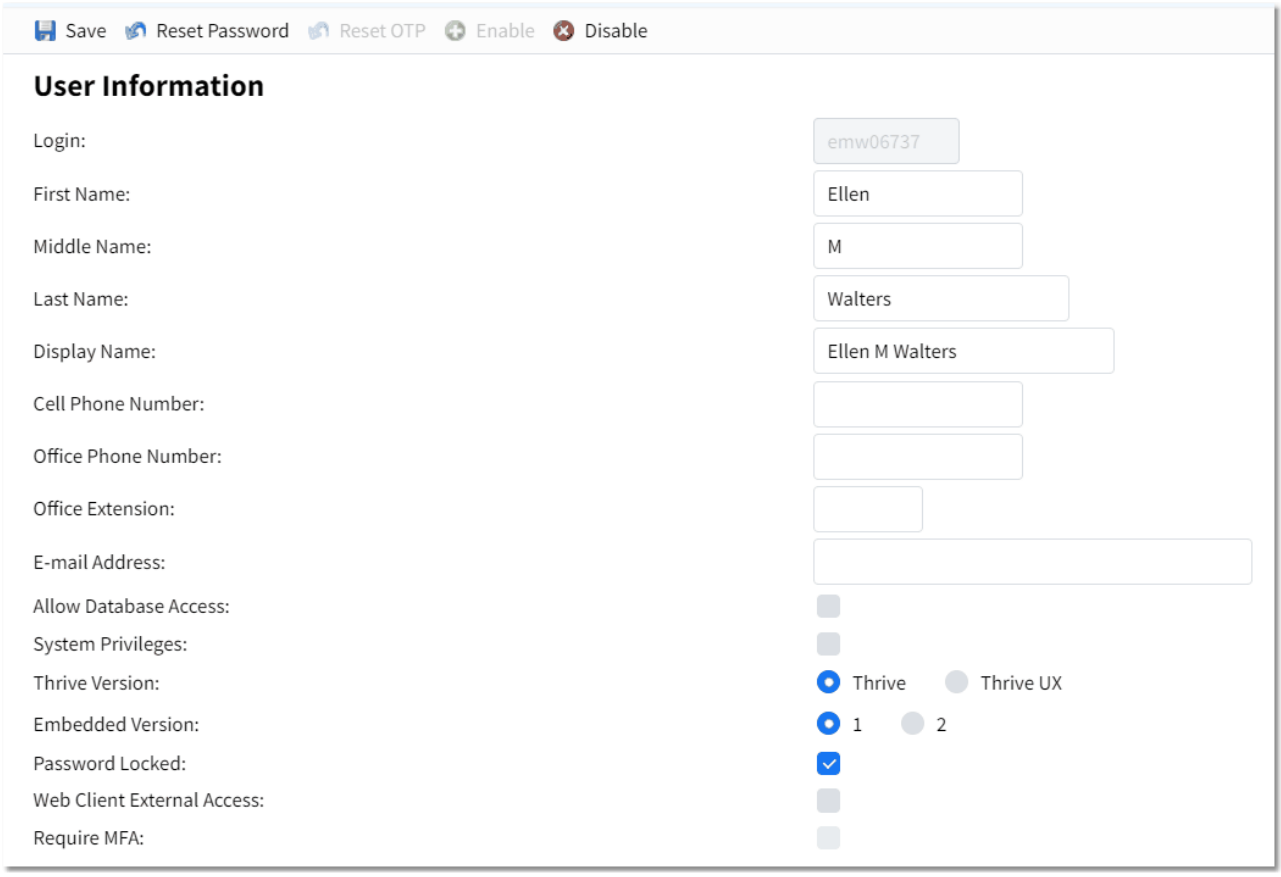


System Administration - Locked Logins

To unlock the user login, select it from the list and then select **Edit** from the action bar.

The User Information screen will then display and will allow the Password Locked field to be unchecked.

Select **Web Client** > **System Administration** > **Logins** > **Show Locked Logins**> **Select a Login** > **Edit**



System Administration - User Information

Once all changes have been made to the User Information screen, select **Save** to save all changes.

The system will then return to the Locked Logins screen. The user login that was unlocked will still display on the Locked Logins screen.

Selecting the **Refresh** option from the action bar will update the screen to reflect the user logins that are still locked.

The **PDF** option may be selected from the action bar to export the information displayed on the screen into a PDF report format.

The **CSV** option may be selected from the action bar to take the information displayed on the screen and export it into Excel.

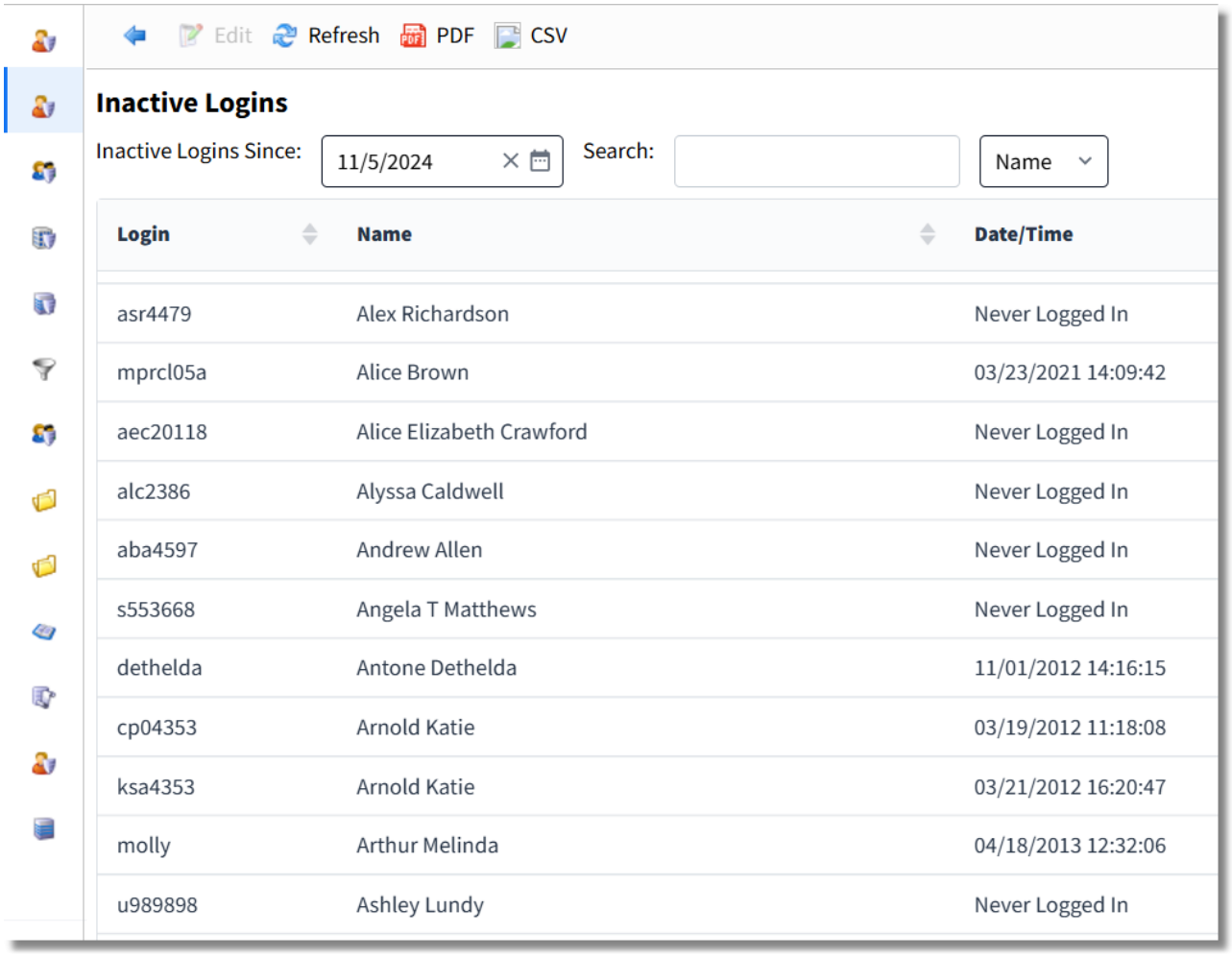
NOTE: *Unlocking an employee's login is the responsibility of the facility's IT department and will not be done by TruBridge.*

Show Inactive Logins

The Show Inactive Logins option will display all enabled logins that have not accessed the system since the date specified. The date will default to 15 days prior to the current date. To view the inactive logins, select **Show Inactive Logins** from the action bar on the Logins screen.

The Inactive Logins screen will display the user Login, the Name associated with the login and the Date/Time that the user last accessed the system.

Select **Web Client** > **System Administration** > **Logins** > **Show Inactive Logins**



Inactive Logins

To disable the user login, select it from the list and then select **Edit** from the action bar.

The User Information screen will then display, from here the Login may be disabled. For more information please see Maintenance 16.

Selecting the **Refresh** option from the action bar will update the screen to reflect the user logins that are still inactive.

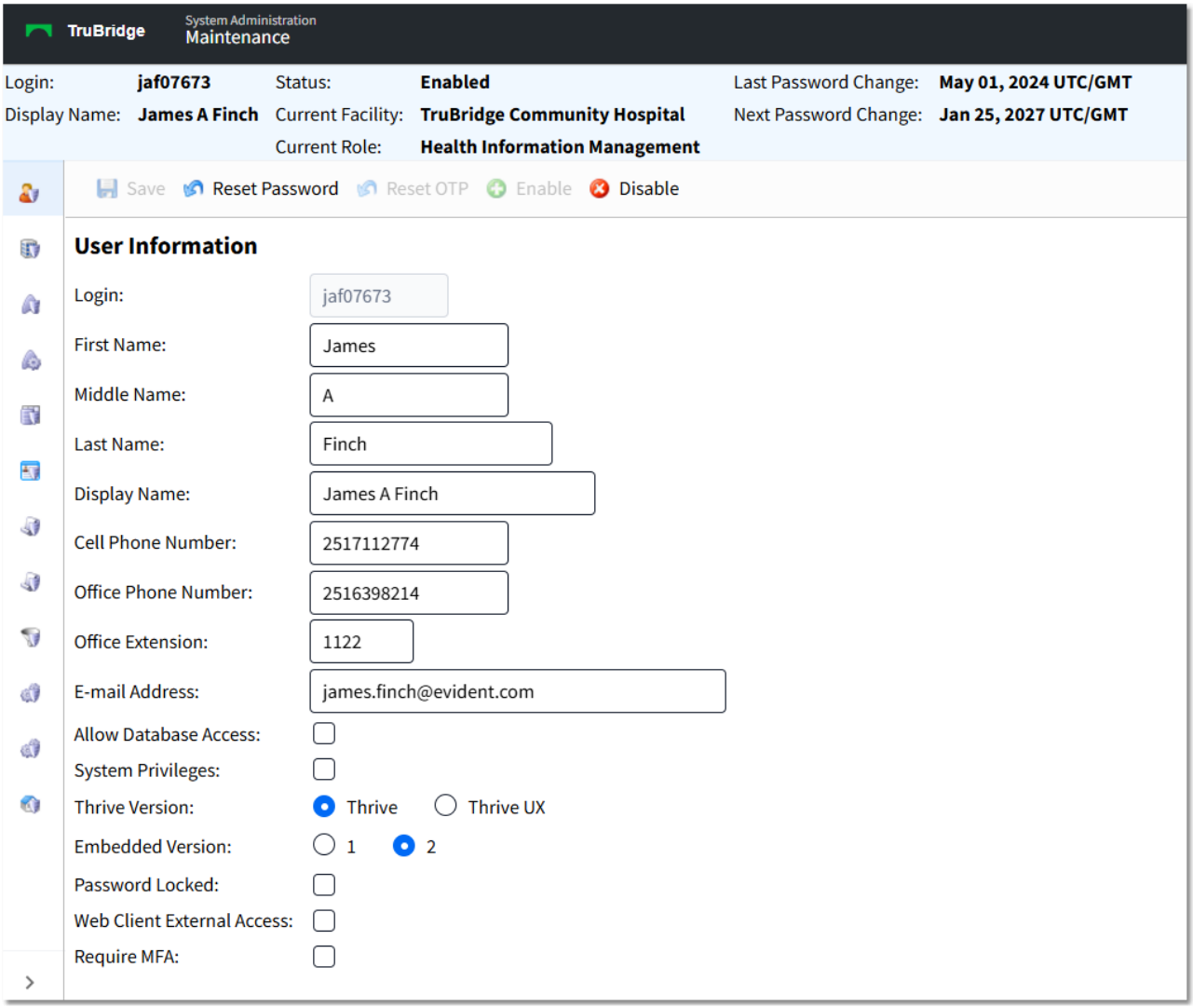
The **PDF** option may be selected from the action bar to export the information displayed on the screen into a PDF report format.

The **CSV** option may be selected from the action bar to take the information displayed on the screen and export it into Excel.

5.1 Maintenance

Once an existing login is selected, the User Information screen will display.

Select **Web Client** > **System Administration** > **Logins** > **Select Login**



System Administration - Users

The following information may be completed for each login.

- **Login:** For existing logins, the logname will be displayed, but the field will be grayed out, and changes will not be allowed. Newly created logins must meet the following criteria:
  - Must not already exist. If the login exists, the user will receive the prompt, "The login is not available. Try another login or call TruBridge Client Services for more information."
  - Range from 3-8 characters in length.
  - The first character must be a lowercase alpha character (a-z).
  - Any additional alpha characters must be lowercase.

- **First Name, Middle Name and Last Name:** Displays the name of the user. Once loaded, the user's name will automatically populate the **Display Name** field.

- **Display Name:** Defines how the user's name and will be displayed throughout the system. This field is automatically populated based on the First, Middle and Last Names but may be changed.

- **Cell Phone Number and Office Phone Number:** Allows the user's contact phone numbers to be entered. Enter only seven or 10-digit numbers without special characters such as dashes or parenthesis. If special characters are loaded, an Invalid Input prompt will display. Select **OK** to acknowledge the Invalid Input prompt and re-enter the number.

- **Office Extension:** Allows up to a 4-digit extension number.

- **E-mail Address:** Allows the user's e-mail address to be entered. If the user's email address matches the email address they used to register for TruLearn, then the user will have a single sign-on experience (won't be required to enter password again) when accessing TruLearn within TruBridge EHR.

- **Allow Database Access:** Determines whether a user can access the system's database. This creates a database login with access to Accounts Receivable, Payroll and/or Accounting with third party software. When selected, the database login will display next to the switch, "Database access given to login *ubl*_db."

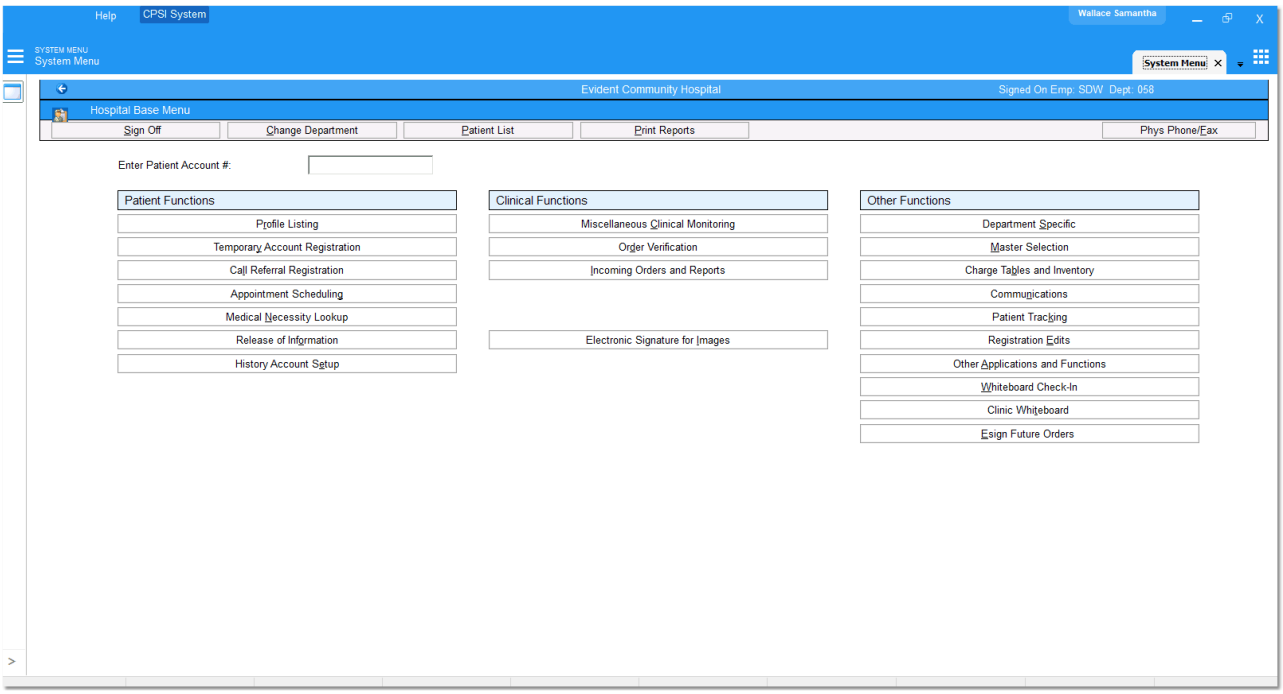
NOTE: *See the DBase 54 section for more information on defining a database login. This option will only be available if ODBC has been purchased. Please contact TruBridge for more information on using this option.*

- **System Privileges:** Selecting System Privileges will allow users, that are not assigned to the System Administrator role, access to create/edit logins, unlock/reset passwords, and modify the system-wide login and password policies. In addition to selecting System Privileges, the user will also need the specific behavior controls to perform these functions. The user will only be able to perform the functions related to the behavior controls they are given. The following behavior controls are associated with these functions:
  - Create and Edit Logins
  - Unlock and Reset Passwords
  - Modify Login and Password Policies.

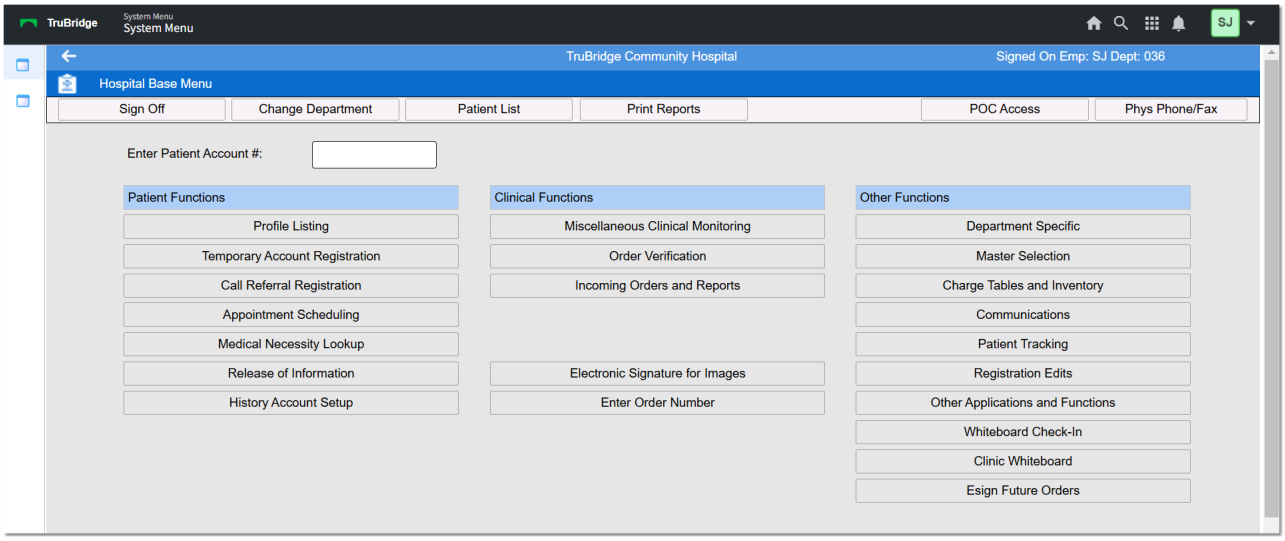
NOTE: *To give a user access to System Privileges, the user assigning the security must be in the System Administrator role. A System Administrator does not have the ability to activate nor deactivate System Privileges for their own login.*

- **Thrive Version:** If Thrive UX is selected, the login will only be able to login using Thrive UX. If Thrive is selected, the user will have the option of choosing Thrive or Thrive UX when signing into the system.

- **Embedded Version**: The embedded version will determine how users will view embedded screens within Thrive UX. See examples below.



Embedded Version 1



Embedded Version 2

- **Password Locked:** Displays the status of the login's password, unlocked (unchecked) or locked (✓). The password will become locked (✓) as a result of a number of attempts greater than the setting for lockout attempts defined in the System Login Policy. The switch may also be manually selected or deselected to lock and unlock the login's password. The Reset Password button will automatically unlock (uncheck) the password as well.

NOTE: *See the System 94 section for more information regarding the Login Policy.*

- **Web Client External Access**: When selected, the user may access the EHR via the Web Client when connecting both in and out of the facility's network. Once selected, the 'Require MFA' option will become available to set for users. When 'Web Client External Access' is not selected, the user may only access the EHR via the Web client when in the facility's network; the user will not be able to access the EHR when out of network. Refer to the Multi-Factor Authentication 135 section for more information.

- **Require MFA (Multi-Factor Authentication)**: When selected, a One-Time Password (OTP) is required when accessing the EHR via the Web Client when connecting out of network. This option is only available when external access to the TruBridge EHR Web Client is allowed (see previous field). When this option is not selected, a OTP is not required when accessing the EHR via the Web Client. Refer to the Multi-Factor Authentication 135 section for more information.

The following options are available on the Action Bar.

- **Save:** Allows changes made to a login to be saved.

- **Reset Password:** Once selected, the Login Password Maintenance screen will display. This will allow the login's password to be reset to either Thrive's Default Password or an "Other" one-time password. When the user accesses Thrive, the password defined here will be used, Thrive will then allow a new password to be set up for the login. The default, or the one-time use reset password, will be hashed using an SHA512 algorithm. This becomes the user's password credential and is stored. Any text keyed in by the system administrator is discarded once the hash is created and stored.

NOTE: *Resetting a user's password is the responsibility of the facility's IT department and will not be done by TruBridge.*

- **Reset OTP:** When selected, the user will receive a new QR Code on their next login attempt. This option will only be enabled when **Require MFA** is selected.

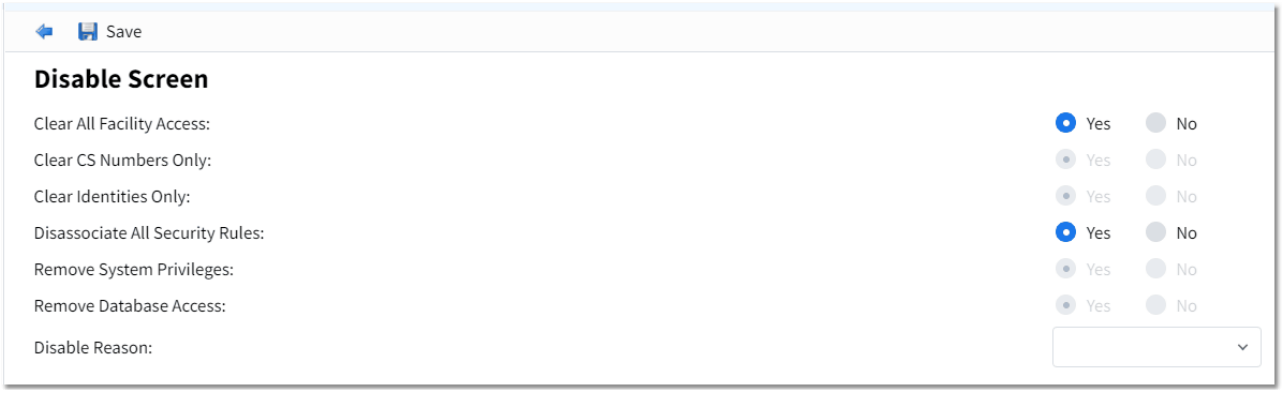
NOTE: *In order to have access to the Reset Password and Reset OTP options, the system admin will need have the Reset and Unlock Password behavior control set to allow.*

- **Enable:** Enabling a user login allows the user to log into the system with that login. Once selected, the Login Password Maintenance screen will display. This will allow the login's password to be reset to either the Thrive's Default Password or an "Other" one-time password. When the user accesses Thrive, the password defined here will be used, Thrive will then allow a new password to be set up for the login.

- **Disable:** Disabling a user login prevents the user from logging into the system with that login. Once disabled, the following will display next to the Login field, "Disabled on *mm/dd/yyyy* by xxxxxxxx." When Disable is selected the Disable Screen will display with additional options for disabling the login. See below for details.

Disable

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Disable**



Disable Screen

The following options are available on the screen.

- **Clear All Facility Access**: If **Yes** is selected, all facility access will be removed from the login. If **No** is selected, all facility access will remain on the login and the options for Clear CS Numbers Only and Clear Identities Only will become available.

- **Clear CS Numbers Only**: If **Yes** is selected, all CS Numbers will be removed from the login. If **No** is selected, the CS Numbers will remain on the login. This option will default to Yes, but it may be changed when Clear All Facility Access is set to No.

- **Clear Identities Only**: If **Yes** is selected, all Employee/Physician numbers will be removed from the login. If **No** is selected, the Employee/Physician numbers will remain on the login. This option will default to Yes, it may be changed when Clear All Facility Access is set to No.

- **Disassociate All Security Rules**: If **Yes** is selected, all Application, Screen, Report, Behavior Control and Event rules will be removed from the login. If **No** is selected, all Application, Screen, Report, Behavior Control and Event rules will remain on the login.

- **Remove System Privileges**: If **Yes** is selected, the System Privileges field on the User Information screen will be unselected when the login is disabled. This will remove the login's ability to perform actions requiring System Privileges. If **No** is selected, System Privileges will remain selected on the User Information screen. This option will be disabled if the user does not have System Privileges selected on the User Information screen.

- **Remove Database Access**: If **Yes** is selected, the Database Access field on the User Information screen will be unselected when the login is disabled. This will remove the login's ability to access the system's database. If **No** is selected, Database Access will remain on the login. This option will be disabled if the user does not have Database Access selected on the User Information screen.

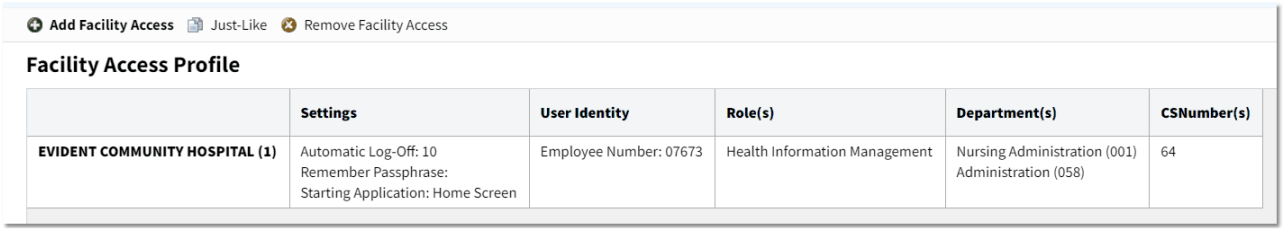
- **Disable Reason:** Allows documenting a reason for disabling a login. Select the desired reason from the drop-down list. These reasons are hard-coded and are as follows:
  - Termination
  - Resignation
  - Retirement
  - Suspension
  - Leave of Absence
  - End of Contract
  - Duplicate Login

Once all fields have been addressed, select **Save**. If the user is currently logged into Thrive, the following prompt will be received, " User xxxxxxxx is logged on. Would you like to end their session?" Answering **Yes** will kill the user's current session and disable the login. Answering **No** will allow the user to continue with their current session until they log out; once logged out, the user's login will be disabled.

5.2 Facility

The Facility screen will need to be completed before the user may log in to the system. Here, the facilities the user will have access to will be defined. For each facility the user's employee number/physician number will be linked, the user's role will be assigned, and what departments the user has access to will be identified.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility**



Facility Access Profile

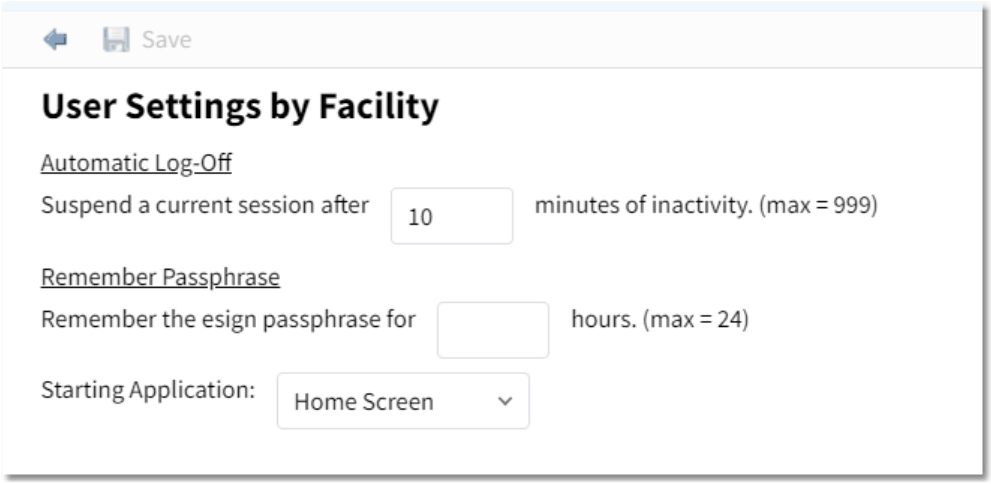
NOTE: *Closing out on any of the following screens will exit the current screen without saving changes.*

NOTE: *Changes to or creating a login will be logged for auditing purposes. This information is stored in the system and can be extracted. Please contact TruBridge support for assistance with this information.*

Settings

Double-click the cell in the **Settings** column to update the settings for a specific facility.

Select **Web Client** > **System Administration** > **Login** > **Settings**



User Settings by Facility

- **Automatic Log-Off**: **Suspend a current session after ___ minutes of inactivity.** The maximum is 999 minutes. The number of minutes of inactivity that must be met before a user is logged off the system. Once logged off, the user will be able to enter their password to resume the session. The Auto Sign-off field in Department Security will override this setting.

- **Remember Passphrase**: **Remember the esign passphrase for ___ hours.** Enter the number of hours the system should remember the passphrase for the role. The maximum is 24 hours.
  - The **Remember Passphrase** behavior will default to one hour.
  - If the role or user has **Remember Passphrase** the system will read the login facility setting value first.
  - If the user facility setting is blank the system will read the role's **Remember Passphrase** facility setting value.

- **Starting Application**: Define the starting application by selecting the desired starting application from the **Starting Application** drop-down menu. The four starting applications are Home Screen, TimeClock, EDistribution and PDA. Home Screen is the default, and will be used for most users logging into Thrive. A TimeClock user login will give direct access to the TimeClock application, EDistribution is used for the Faxing application, and PDA is used with the Materials Management application.

Select **Save** after setting the User Settings by Facility.

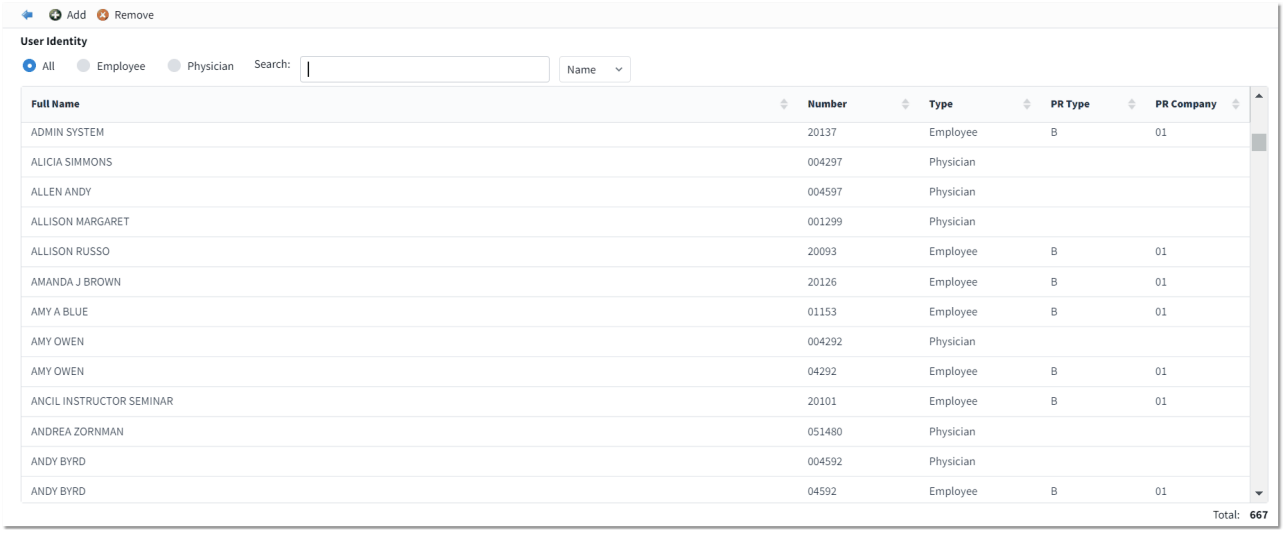
User Identity

User Identity is used to assign the user's employee number or physician number to the login. Adding a user identity will link the traditional security settings for the user to the login. Traditional security settings still determine access in certain areas of Thrive; these security settings are setup in the following location: Web Client > System Menu > Special Functions > System Management > System Security > Employee Security/Physician Security.

To assign an employee number/physician number to a login, complete the steps below.

1. Select the cell in the **User Identity** column for the desired facility. The User Identity look-up table will be displayed with the user's full name, employee or physician number and the type of user, Employee or Physician.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select User Identity**



User Identity

2. Select the desired employee or physician. A search option is displayed at the top of the screen to search for users by either Name or Number. Radio buttons are also available to delimit the search for **All**, **Employee** or **Physician** users. The default will be **All** by Name.

3. Select **Add**.

An employee number may be associated with more than one login. If the selected employee number is already tied to a login, then the system will prompt "That identity is already tied to login xxxx. Would you like to continue?"; answering **Yes** to this prompt will allow the employee number to be tied to an additional login.

A physician number may only be associated to one login. If the selected physician number is already tied to a login, then the system will prompt "That identity is already tied to login xxxx. Please select another identity; selecting **Ok** to this prompt will return the user to the User Identity list to choose a number that is not currently associated with a login.

User identities for terminated employees or physicians will not display in the User Identity look-up table.

To remove an employee or physician number from an existing login, select **Remove** from the action bar.

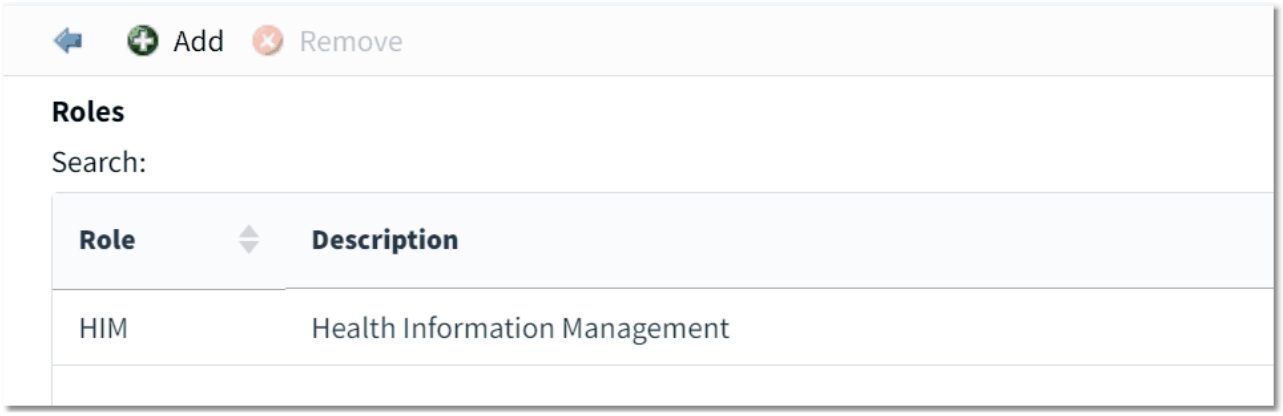
Role(s)

Assigning a Role to a login is an important part of login setup. All logins must be assigned to a role and each login may only be assigned to one role. Security rules may be setup on the role, so when a role is assigned to the login, it provides a baseline for the user's security access.

Complete the following steps to assign the user's role.

1. Double-click the cell in the **Role(s)** column for the desired facility.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select Role(s)**

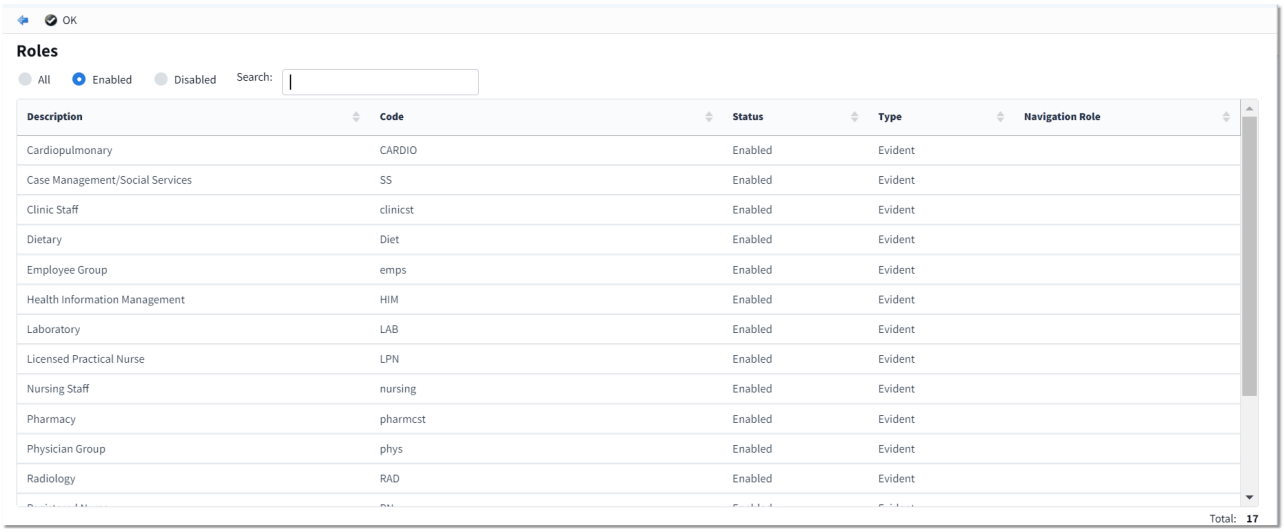


Roles

2. Select **Add**. The list of available Roles and their codes will display.

***NOTE**: TruBridge Default roles are available to choose from; however, custom roles may be created as well. For information on creating custom roles, please review the Roles 64 section of this User Guide.*

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select Role(s)** > **Add**



Roles List

3. Select the desired Role.
4. Select **OK**.

Only one role may be assigned to a login. If a login already has a role defined, then selecting a new role will overwrite the original role.

To remove a Role from a login:

1. Select the cell in the **Role(s)** column for the desired facility.
2. Select the Role to be removed.
3. Select **Remove**.

Department(s)

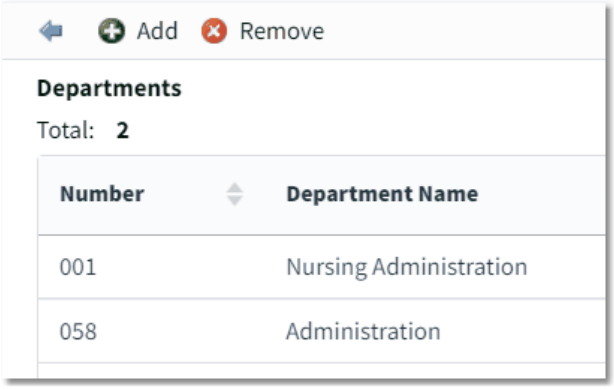
Assigning departments to a login will determine what departments the user will have access to in the system. The users will only have access to the departments in this column. When changing departments, the departments listed here will be available for the user to choose from.

If no departments are entered (Department column is left blank), the user will be required to enter a department password when changing departments. If the password is unknown the user will not be able to access the department.

To assign a department to a login:

1. Double-click the cell in the **Department(s)** column for the desired facility.

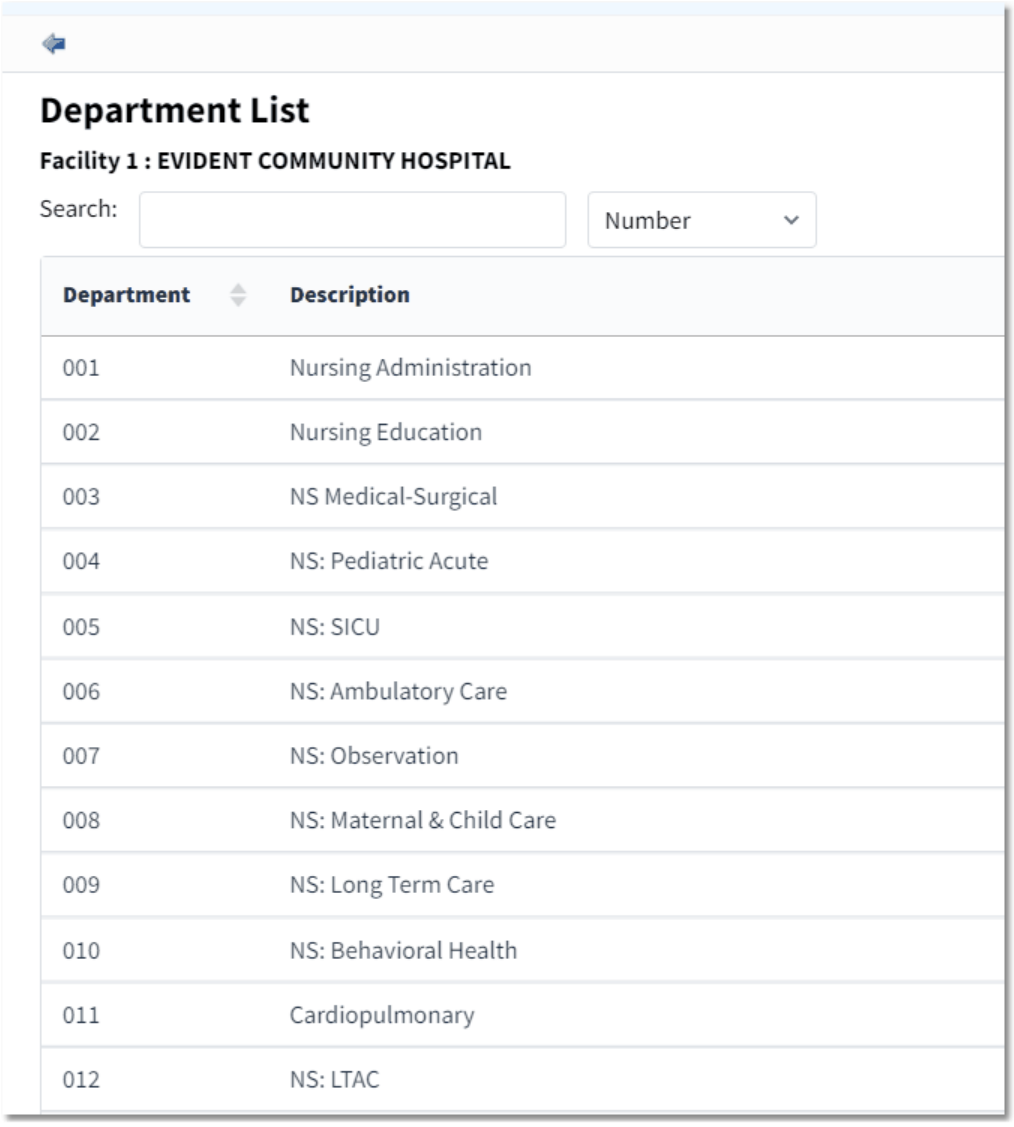
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select Department(s)**



Departments

2. Select **Add**. The list of Departments and their department numbers will display. A search option is displayed at the top of the screen to search for departments by either Number or Description. The default is by Number.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select Department(s)** > **Add**



Department List

3. Select the desired Department.

Repeat steps two and three to add multiple departments.

To remove a department from a login:

1. Select the cell in the **Department(s)** column for the desired facility.
2. Select the Department to be removed.
3. Select **Remove**.

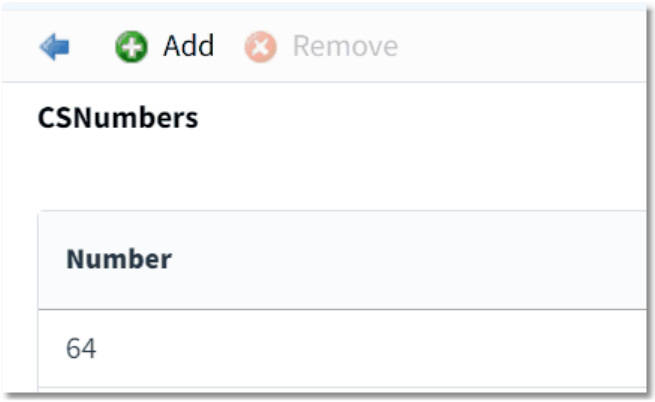
CSNumber(s)

CS Numbers are used throughout the system to track specific transactions. While a CS Number is not required for a login, it is recommended that CS Numbers be assigned to logins that perform the following functions: cash posting, receipt posting, closing days in Accounts Receivable, insurance billing, statement processing, Accounts Payable, General Ledger, and advanced ad hoc reporting.

To assign a CSNumber to a login:

1. Select the cell in the **CSNumber(s)** column for the desired facility.

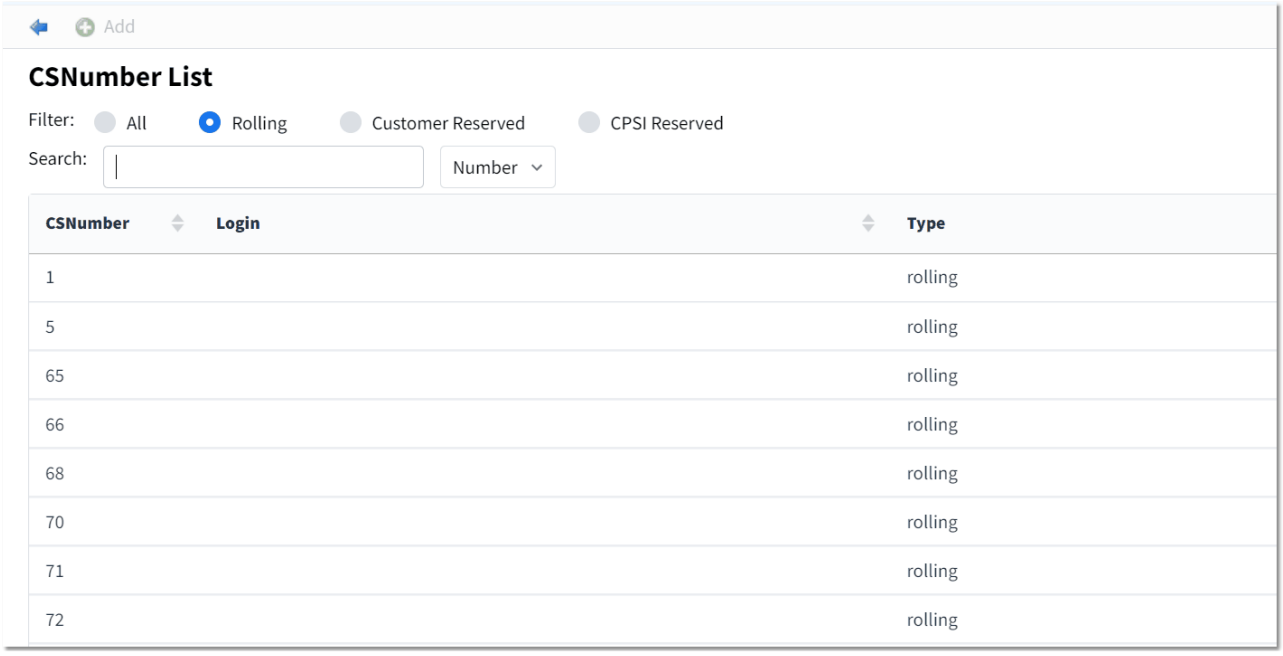
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select CSNumber(s)**



CSNumbers

2. Select **Add**. The list of available CSNumbers with login and type will display. Radio buttons are available to delimit the search for **All**, **Rolling**, **Customer Reserved** or **CPSI Reserved**. A search option is also displayed at the top of the screen to search for CSNumbers by either Number or Type. The default is **Rolling** by Number.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Select CSNumber(s)** > **Add**



CSNumber List

3. Select the desired CSNumber.
4. Select **Add**.

Only one CSNumber may be assigned to a login. If a login already has a CSNumber defined, then selecting a new CSNumber will overwrite the original CSNumber.

When delimited by **Rolling**, logins will display for those CSNumbers that are currently in use. Once a CSNumber is associated with a login, it will no longer be found under the **Rolling** filter. All assigned CSNumbers will be listed under the **Customer Reserved** filter and will display with the associated login.

To remove a CSNumber from a login:

1. Select the cell in the **CSNumber(s)** column for the desired facility.
2. Select the CSNumber to be removed.
3. Select **Remove**. The CSNumber will revert back to rolling.

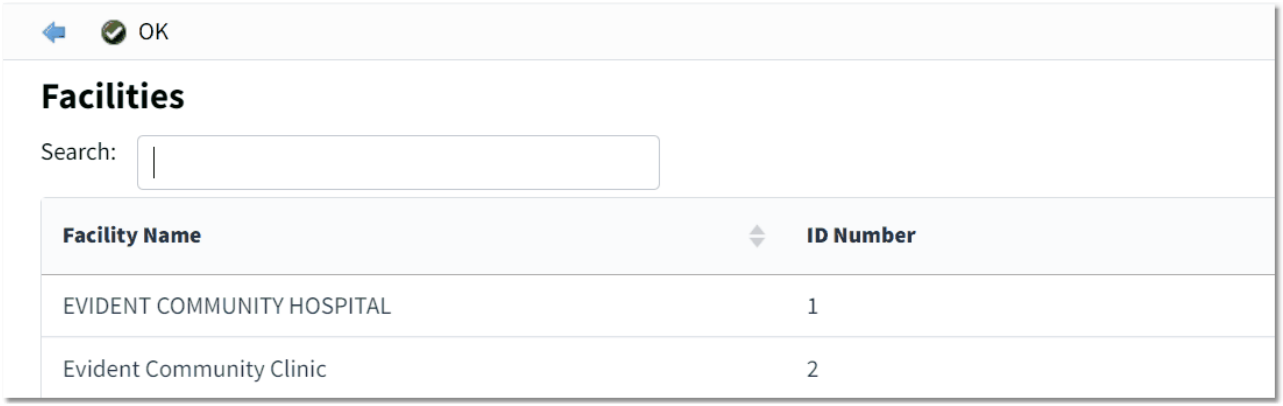
Add/Remove Facility Access and Just-Like

Each user login may be attached to several facilities.

To attach a facility to a login:

1. Select **Add Facility Access** from the action bar.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Add Facility Access**



Facilities - Facility Search

2. Select the desired facility to add.
3. Select **OK**.

To remove a facility from a login:

1. Select **Remove Facility Access**.
2. Select the desired facility to remove.
3. Select **OK**.

Just-Like

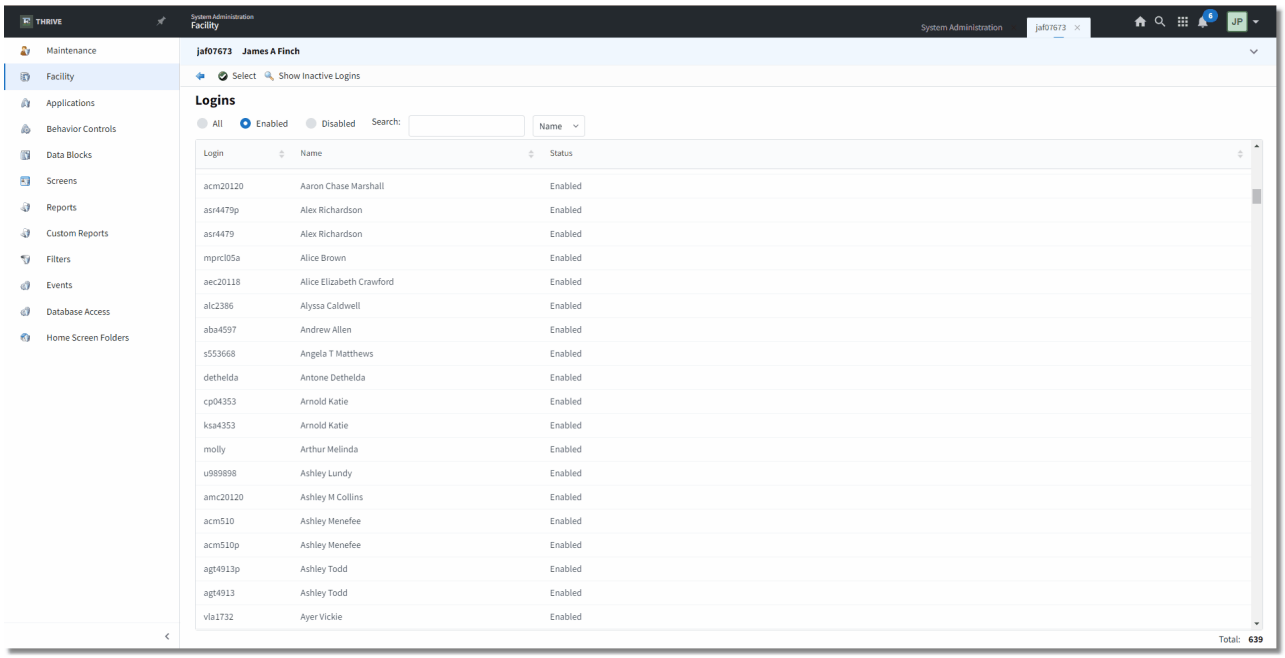
The Just-Like option will allow the facility settings to be copied from another user. When performing a just-like function, all facilities, starting applications, roles and departments will be copied into the login. User Identity will be blank, and CSNumber(s) will default to "rolling." Both areas will need to be defined as needed.

***NOTE**: The Just-Like option does not copy security rules. To assign existing security rule to a login, use the Rule Management feature.*

To just-like the facility settings from another login:

1. Select **Just-Like**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Facility** > **Just-Like**



Just-Like - Login Search

2. Select the desired employee. Possible searches include **All** logins, **Enabled** logins and **Disabled** logins. These may be searched by Name or Login. The default is **Enabled** by Name.

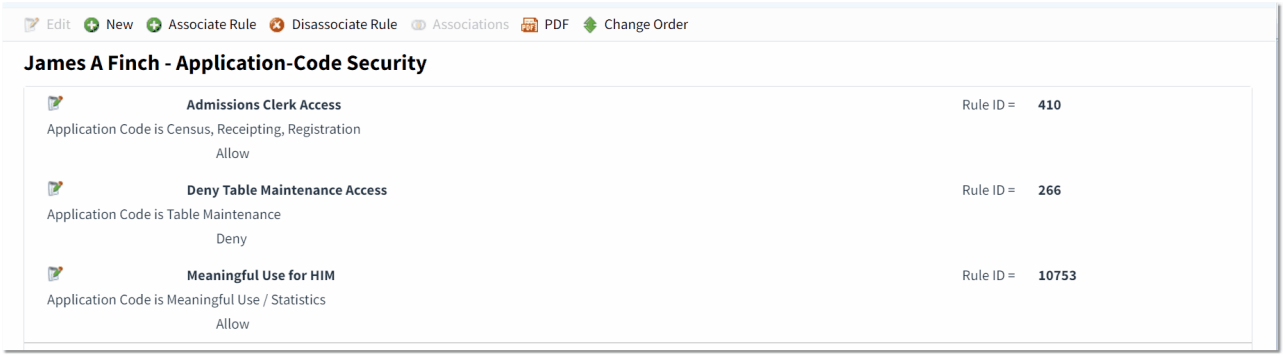
3. Choose **Select**.

5.3 Applications

The Application rules determine what applications the user has access to. All CW5 screens and report templates are tied to an application; so allowing or denying access to a specific application will allow/deny access to all the screens and reports that belong to that application. Rules may only be set up for applications that have been turned on for a facility.

When **Applications** is selected, all security that is currently set up will display. If a rule already exists, it may be modified by selecting it from the screen. The screen will be blank if no rules have been set up for this login.

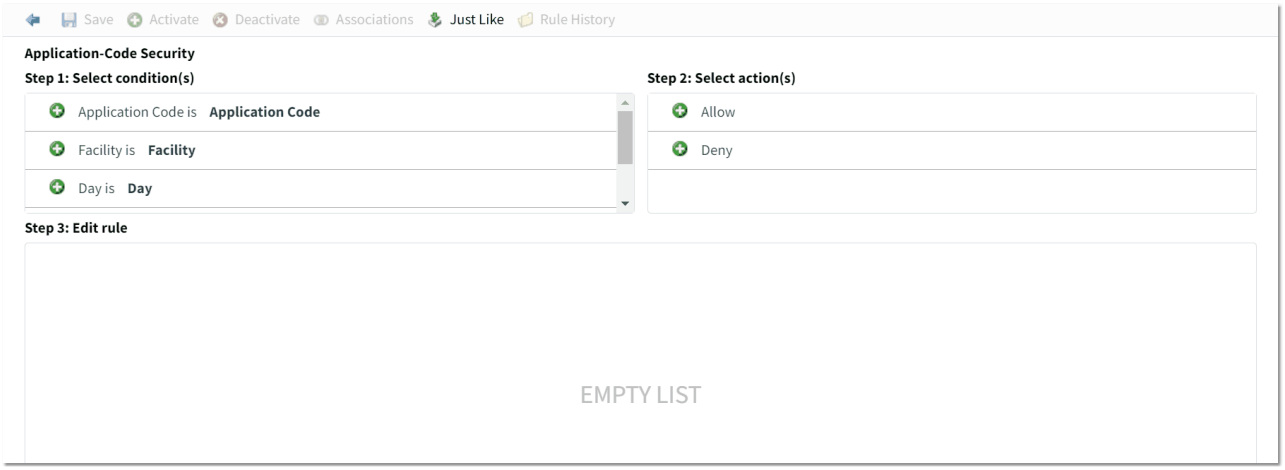
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Applications**



Applications

To set up a new rule, select **New** from the action bar. Or select an existing rule and select **Edit**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Applications** > **New**

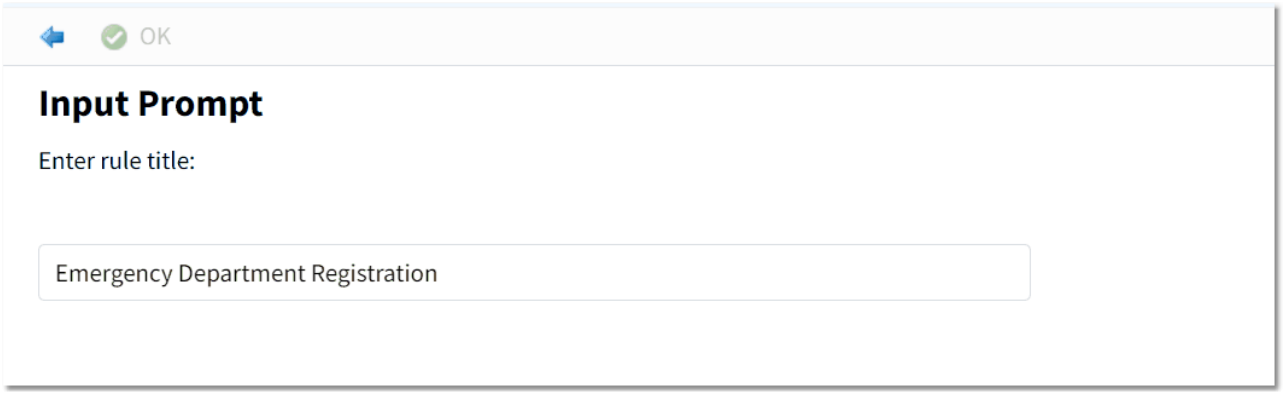


Application

The rule builder screen will then display. Each rule must have a Title. To assign a title to the rule, select the text "**Application-Code Security**." Enter the rule title, then select **OK**.

***NOTE**: If a rule title is not entered when the rule is saved, the user will be prompted to enter a title when exiting the rule builder screen. A title must be entered before the rule may be saved.*

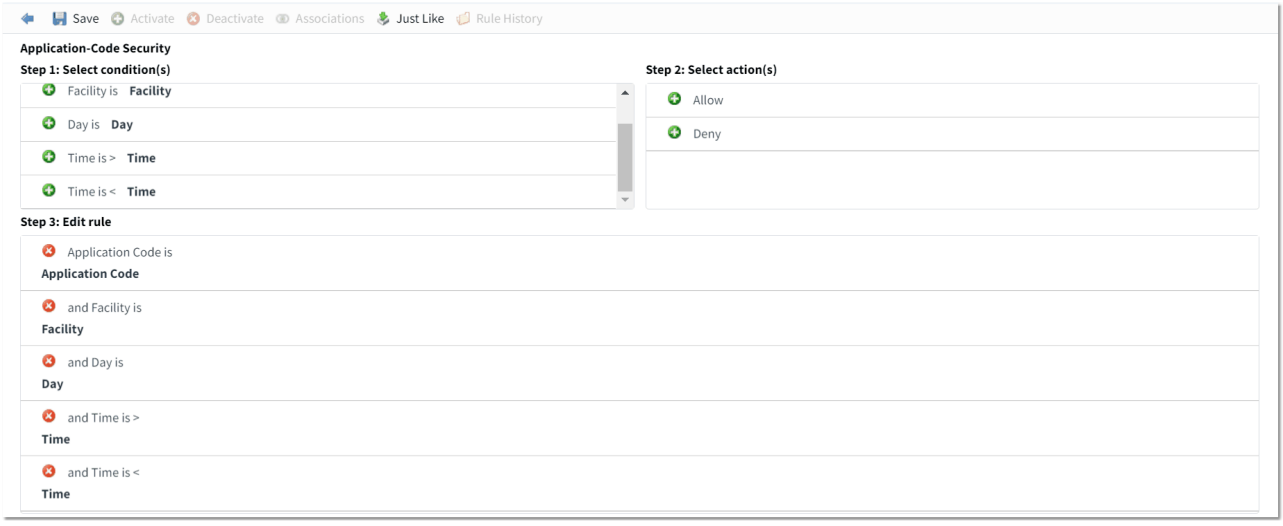
Select **Web Client > System Administration > Logins > Select Login > App > New > Application-Code Security**



Application

In **Step 1**, select the conditions for the rule. The possible conditions include: the Applications that may be accessed, the facilities that may be accessed, the days of the week in which access will be allowed, and an allowable time range for access. For more information on setting up conditions please see Facility 36, Day(s) 37, Start Time 38, End Time 38.

Select **Web Client > System Administration > Logins > Select Login > App > New > Select Condition(s)**

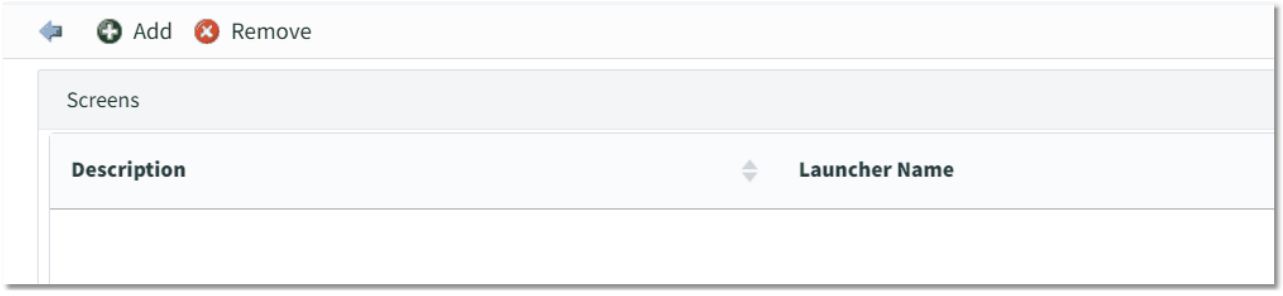


Application - Step 1

In **Step 2**, select the action for the rule. Select the **green plus sign** next to Allow user access or Deny user access. Whichever option is selected in **Step 2**, will then be reflected in **Step 3**. To remove the selected action, select the red X minus sign will remove the action from **Step 3**.

Once a condition and action have been selected, the rule may be edited in **Step 3**. To do this, select the words that are in bold lettering (i.e. Application Code, Facility, Day(s), Start Time, End Time.)

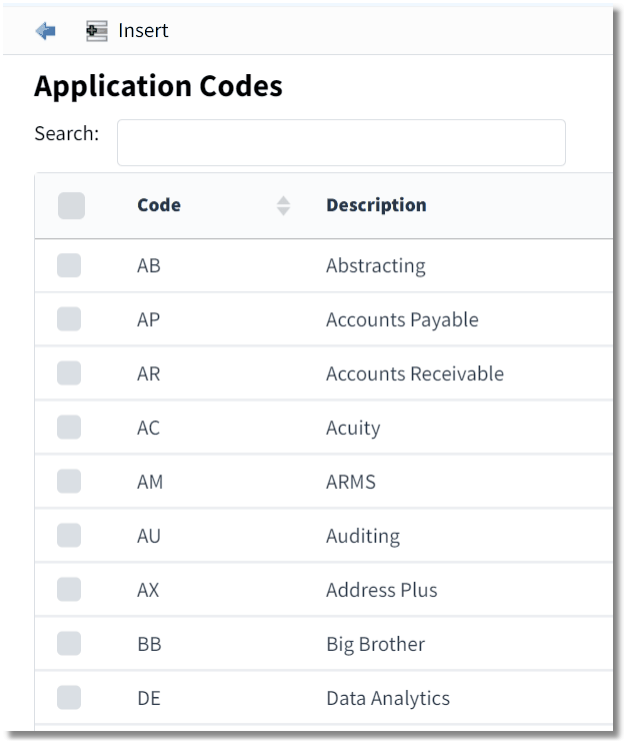
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **App** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit The Rule Description**



Application Code

Selecting the word "**Application Code**", in **Step 3**, allows the creation of a single rule for all applications that have the same authorization, rather than being forced to have individual rules for each application. Application codes that have already been selected will display on the Selected Application Codes screen. If applications already exist, they may be modified by selecting them from the list. To add an application, select **Add** from the action bar. To remove an application code from this screen, select the application so that it is highlighted in blue, and then select **Remove** from the action bar.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **App** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit The Rule Description** > **Add**



Application Code

If **Add** was selected, the screen will display all applications in CW5 or applications that have an associated Report Writer template. Select the application(s) the rule applies so that it is highlighted in blue. Multiple applications may be selected by holding the Ctrl button and selecting each application to add. Then select **Insert** from the action bar.

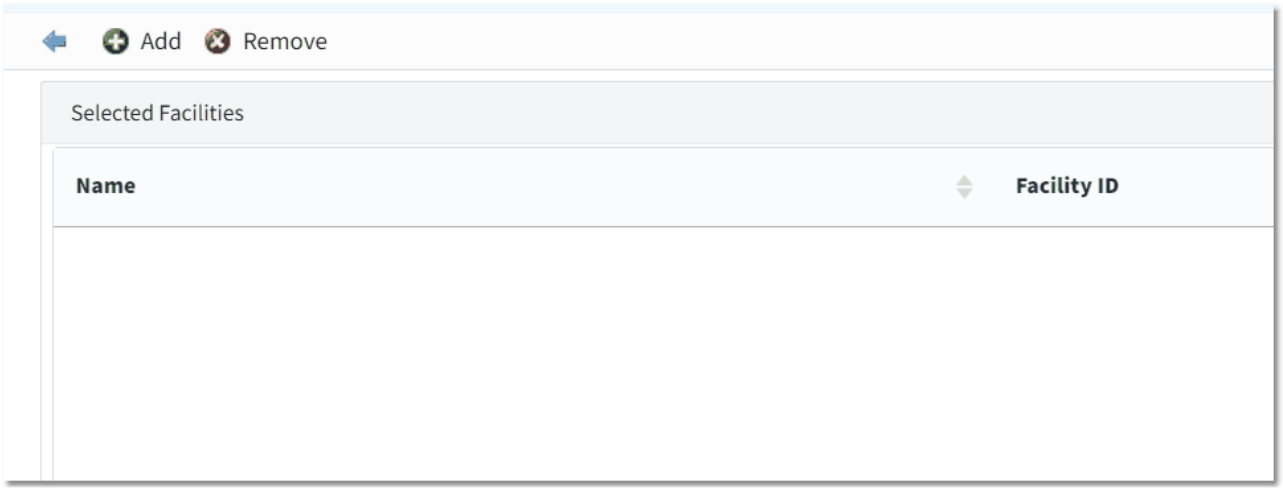
Once **Insert** is selected, the system will go back to the Selected Application Codes screen. To go back to the Rules screen, select the **back arrow** from the action bar.

Facility

Using Facility as a condition of a rule will allow access to be defined differently for a specific facility.

After selecting the word **Facility** in **Step 3**, the Selected Facilities screen will display showing facilities that have already been selected. To add a facility, select **Add** from the action bar.

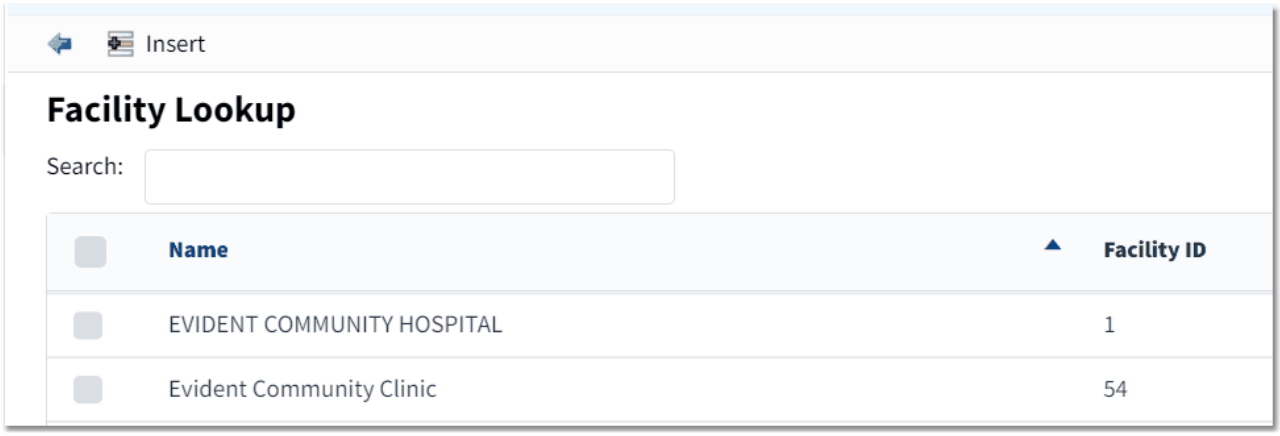
Select **System Administration > Logins > Select Login > Select Application/Behavior Controls/Screens/Report > New > Select Condition(s) > Select Action(s) > Edit The Rule Description**



Facility

A screen will then display a listing of all facilities set up in the Facility ID Table.

Select **System Administration** > **Logins** > **Select Login** > **Select Application/Behavior Controls/Screens/Report** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit The Rule Description** > **Add**



Facility

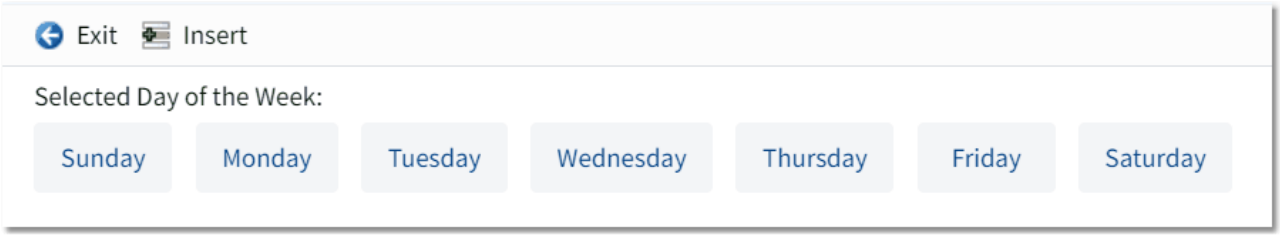
Select the facility that the rule applies to. Then select **Insert** from the action bar. Once the Insert option has been selected, the system will go back to the Selected Facilities screen. To go back to the Rules screen, select the **back arrow** from the action bar.

Day

Using Day as a condition of a rule will allow access to be defined differently for each day of a week.

Selecting the **Day** option in **Step 3** will allow individual days of the week to be selected.

Select **System Administration** > **Logins** > **Select Login** > **Select Application/Behavior Controls/Screens/Report** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit The Rule Description**



Days of Week

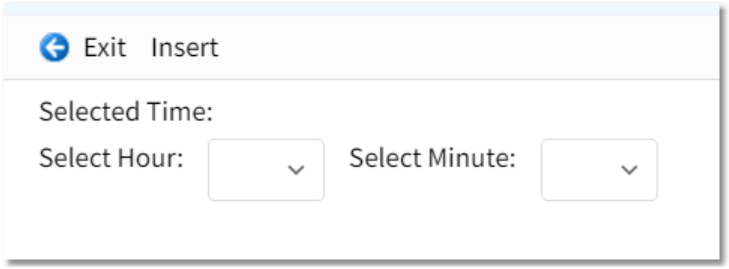
Select the days of the week in which the item may be accessed. As the days are selected, they will display next to the "Selected Day of the Week" field. Once all the days have been chosen, select **Insert** from the action bar. Once Insert has been selected, the system will go back to the Rules screen. Select **Exit** from the action bar to exit without saving.

Start Time

Using Start Time as a condition of a rule will allow access to be defined differently for specific time frames.

Selecting the word **Time** for Time is > in **Step 3** will allow a start time to be selected for the rule.

Select **System Administration > Logins > Select Login > Select Application/Behavior Controls/Screens/Report > New > Select Condition(s) > Select Action(s) > Edit The Rule Description**



Start Time

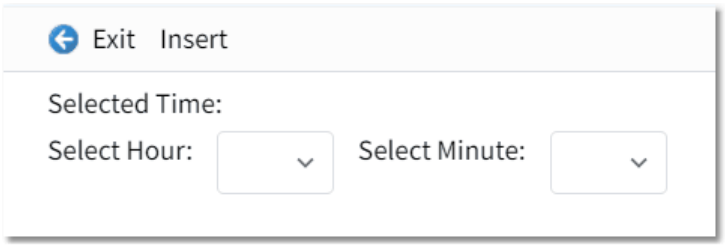
Select a beginning Hour and Minute in which the screen(s) may be accessed. Once the beginning time has been chosen, select **Insert** from the action bar. Once Insert has been selected, the system will go back to the Rules screen.

End Time

Using End Time as a condition of a rule will allow access to be defined differently for specific time frames.

Selecting the word **Time** for Time is < in **Step 3** will allow an end time to be selected for the rule.

Select **System Administration > Logins > Select Login > Select Application/Behavior Controls/Screens/Report > New > Select Condition(s) > Select Action(s) > Edit The Rule Description**

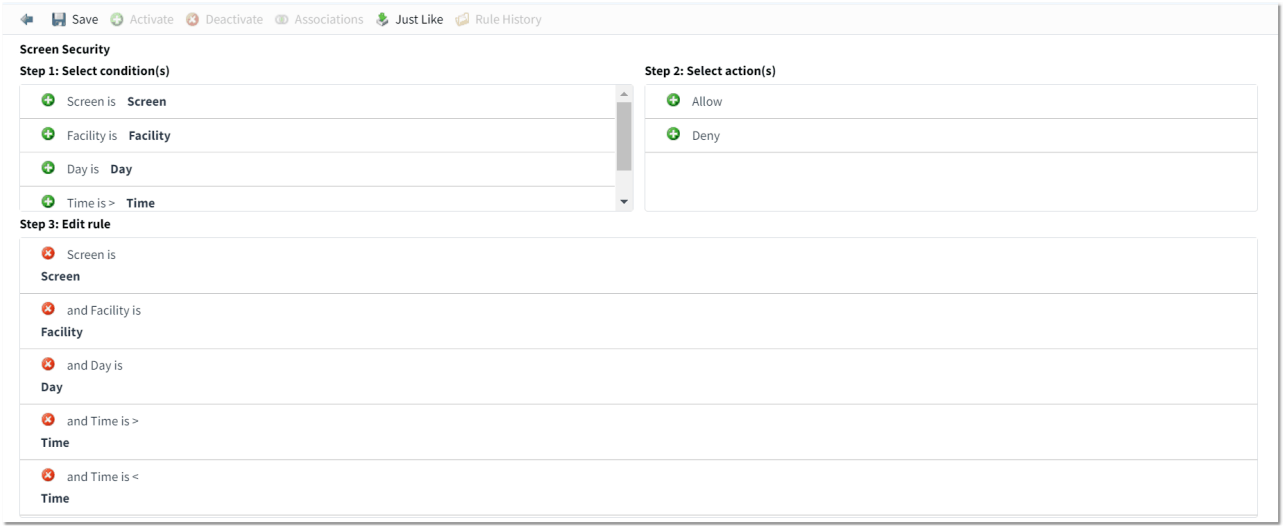


Stop Time

Select the ending Hour and Minute in which the item will no longer be able to be accessed. Once the ending time has been chosen, select **Insert** from the action bar. Once Insert has been selected, the system will go back to the Rules screen.

NOTE: *Military Time is used to denote time.*

Select **System Administration > Logins > Select Login > Select Application/Behavior Controls/Screens/Report > New > Select Condition(s) > Select Action(s) > Edit The Rule Description > Select Hour/Minute > Insert**



Application Rule Builder

Once all the conditions have been defined, the screen will resemble the screen included above. To save the information listed in this screen, select **Save** from the action bar. To exit the screen, select the back arrow at the bottom the screen.

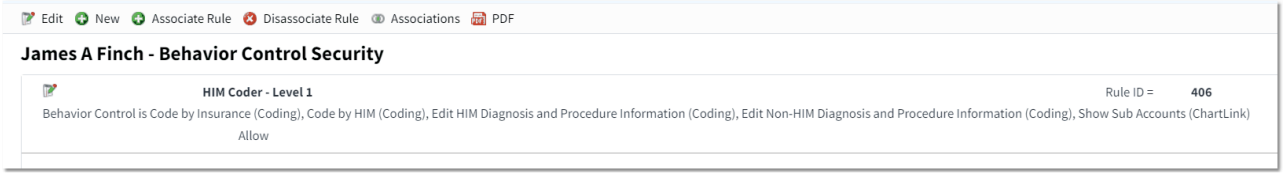
If another rule needs to be set up for another application, screen or report, select **New** from the action bar.

5.4 Behavior Control

Behavior Control rules define what actions a user may take within an application (screen or report). For a definition of what each behavior control does within Thrive, please see the Behavior Control Definitions section of this user guide.

If a rule already exists, it may be modified by selecting it from the screen. The screen will be blank if no rules have been set up for the application.

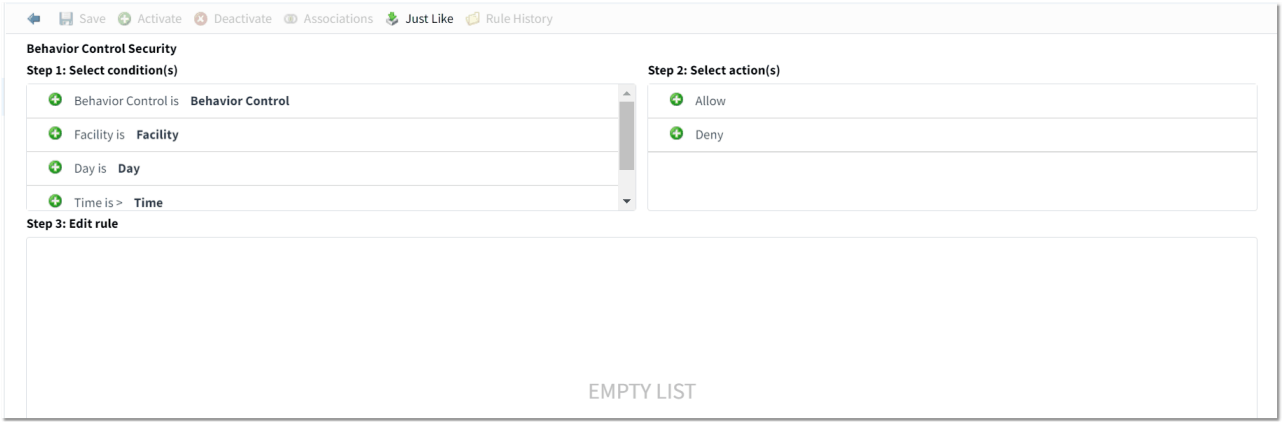
Select **Web Client > System Administration > Logins > Select Login > Select Behavior Controls**



System Administration - Behavior Control

To set up a new rule, select **New**. Or select an existing rule and select **Edit**. The rule builder screen will then display.

Select **Web Client** > **System Administration** > **Select Login** > **Select Behavior Control** > **New**

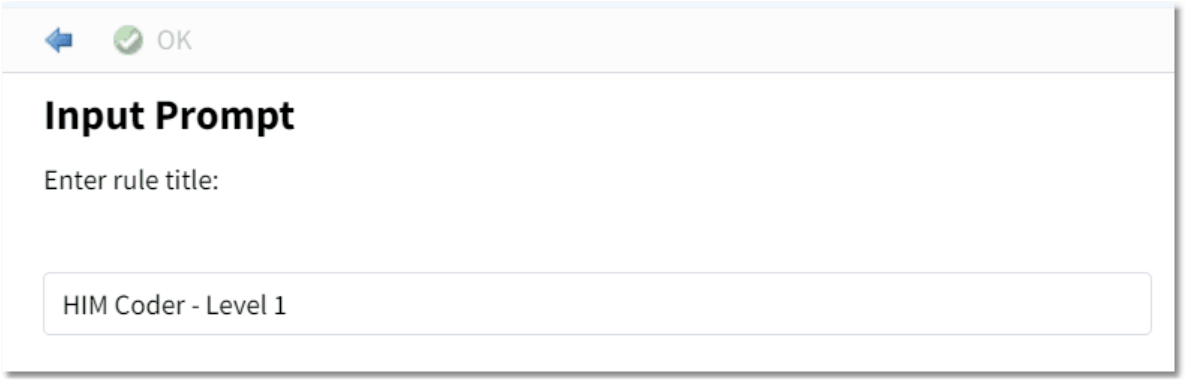


System Administration - Behavior Control

Each rule that is set up must have a Title. To assign a title to the rule select the text "**Behavior Control Security**." Enter the rule title, then select **Ok**.

***NOTE**: If a rule title is not entered when the rule is saved, the user will be prompted to enter a title when exiting the rule builder screen. A title must be entered before the rule may be saved.*

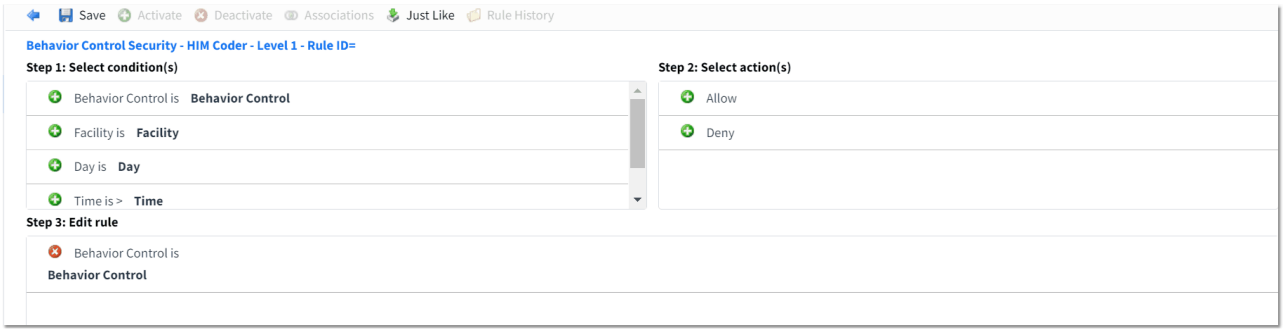
Select **Web Client** > **System Administration** > **Select Login** > **Select Behavior Control** > **New** > **Behavior Control Security**



System Administration - Behavior Control

In **Step 1**, select the conditions for the rule. The possible conditions include: the Applications that may be accessed, the facilities that may be accessed, the days of the week in which access will be allowed, and an allowable time range for access. For more information on setting up conditions please see Facility 36, Day(s) 37, Start Time 38, End Time 38.

Select **Web Client** > **System Administration** > **Select Login** > **Select Behavior Control** > **New**

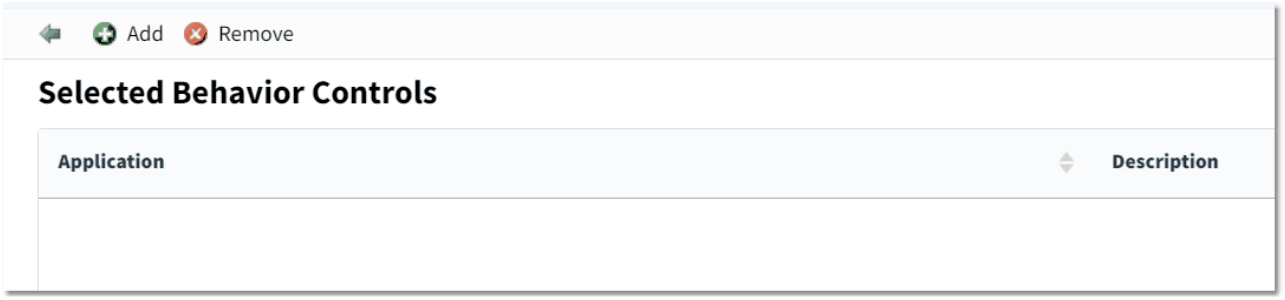


System Administration - Behavior Control

In **Step 2**, select the action for the rule. Select the **green plus sign** next to Allow user access or Deny user access.

Once a condition and action have been selected, the rule may be edited in **Step 3**. To do this, select the words in bold lettering (i.e. Behavior Option, Facility, Day, Time)

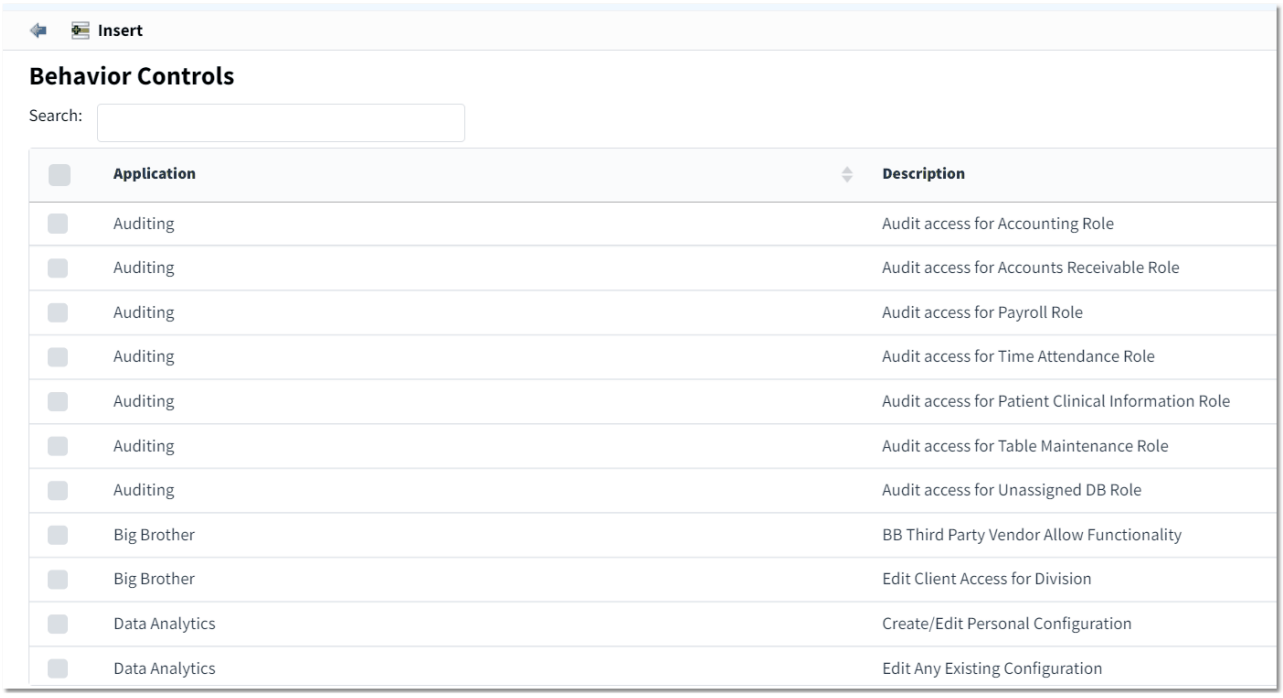
Select **Web Client** > **System Administration** > **Select Login** > **Select Behavior Control** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit Behavior Control**



System Administration - Behavior Control Options

When selecting the word "**Behavior Control"** in **Step 3**, the Selected Behavior Control will display showing any behaviors that already have rules created for them. If a rule already exists, it may be modified by selecting it from the screen. To add a rule for the behavior, select **Add** from the action bar. To remove a rule from the screen, select it so that it is highlighted in blue, then select **Remove** from the action bar.

Select **Web Client > System Administration > Select Login > Select Behavior Control > New > Select Condition(s) > Select Action(s) > Edit Behavior Control > Add**



System Administration - Behavior Controls

If **Add** was selected, select the behavior(s) that the rule is for, so that it is highlighted in blue. Then select **Insert** from the action bar.

Once **Insert** is selected, the system will go back to the Selected Behavior Controls screen. To go back to the Rule Builder screen, select the **back arrow** from the action bar. To save the information listed in the Rule Builder screen, select **Save** from the action bar. To exit the screen, select the **back arrow**.

5.5 Data Blocks

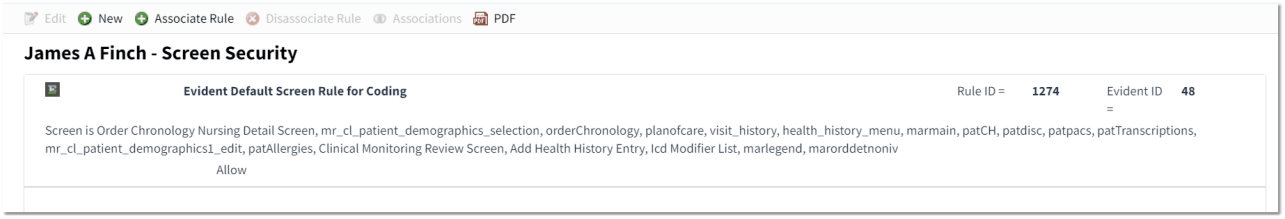
This feature is used with the Data Mining application. Please see the Data Mining user guide for more information.

5.6 Screens

Screen rules define specific screens a user may access. Screen rules apply to those screens using CW5 functionality.

When **Screen** is selected, all security that has already been set up will display. If a rule has not been set up, the screen will be blank.

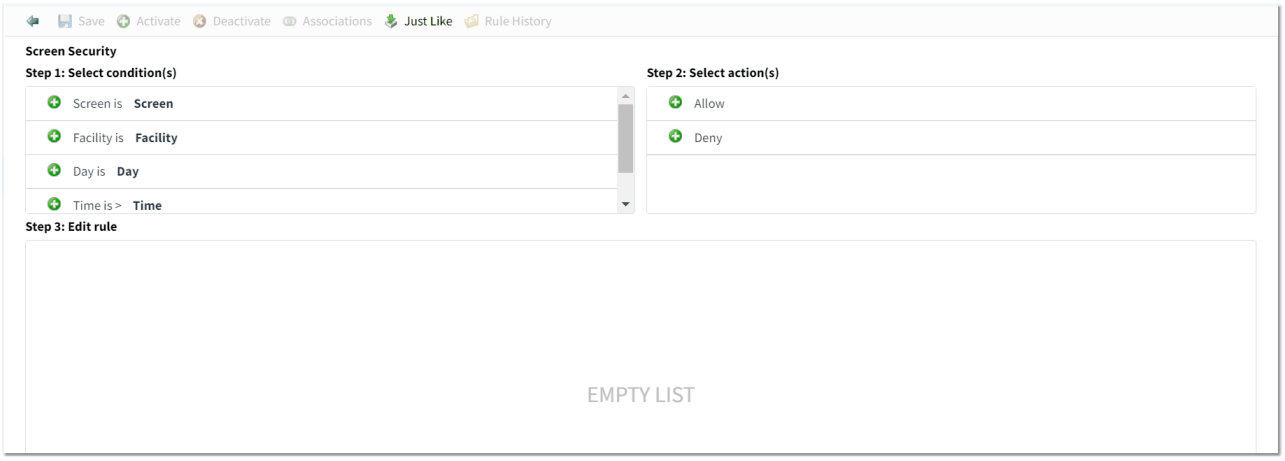
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Screens**



System Administration - Screens

To set up a new rule for Screen Security, select **New** from the action bar. Or select an existing rule and select **Edit**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Screens** > **New**

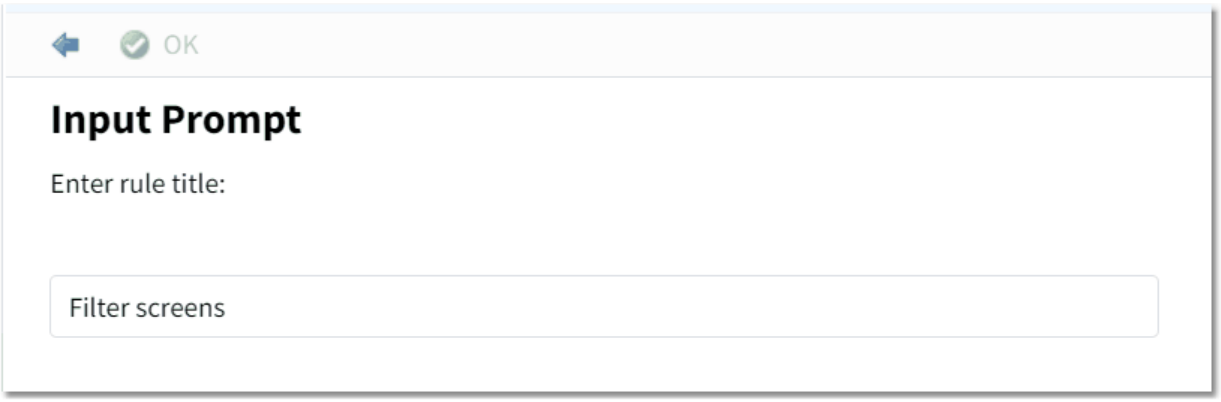


System Administration - Screens

The rule builder screen will display. Each rule must have a Title. To assign a title to the rule, select the text "**Screen Security**." Enter the rule title, then select **Ok**.

***NOTE**: If a rule title is not entered when the rule is saved, the user will be prompted to enter a title when exiting the rule builder screen. A title must be entered before the rule may be saved.*

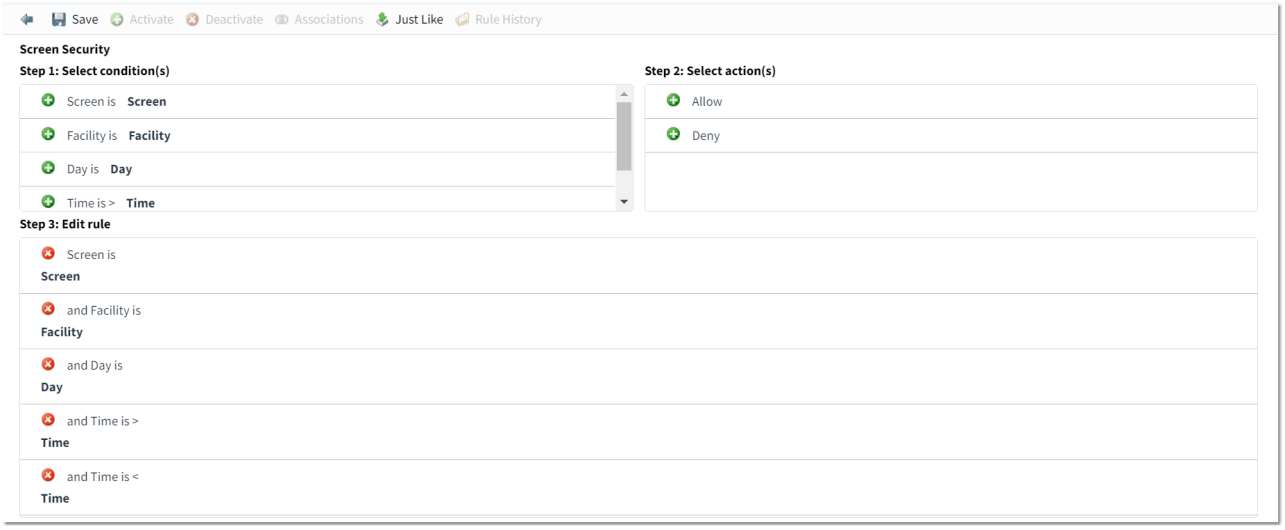
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Screens** > **New** > **Screen Security**



System Administration - Screens

In **Step 1**, select the conditions for the rule. The possible conditions include: screens that may be accessed, facilities that may be accessed, days of the week in which access will be allowed, and an allowable time range for access. For more information on setting up conditions please see Facility 36, Day(s) 37, Start Time 38, End Time 38.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Screens** > **New**

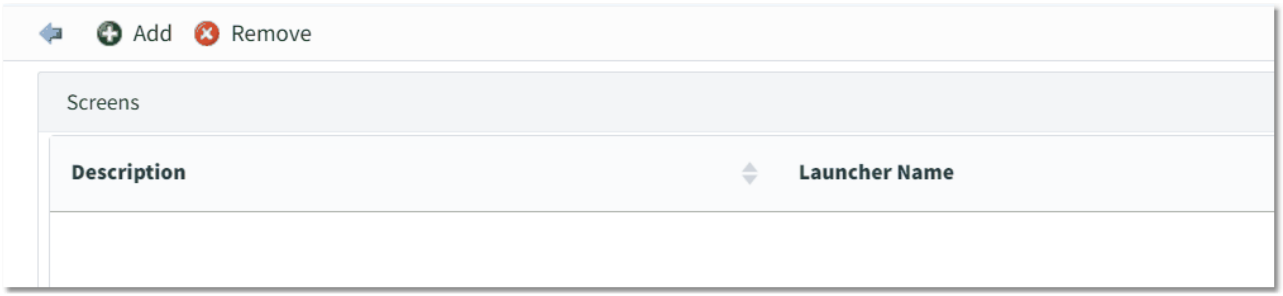


System Administration - Screens

In **Step 2**, select the action for the rule. Select the **green plus sign** next to Allow user access or Deny user access.

Once a condition and action have been selected, the rule may be edited in **Step 3**. To do this, select the words in bold lettering (i.e. Screen, Facility, Day, Time)

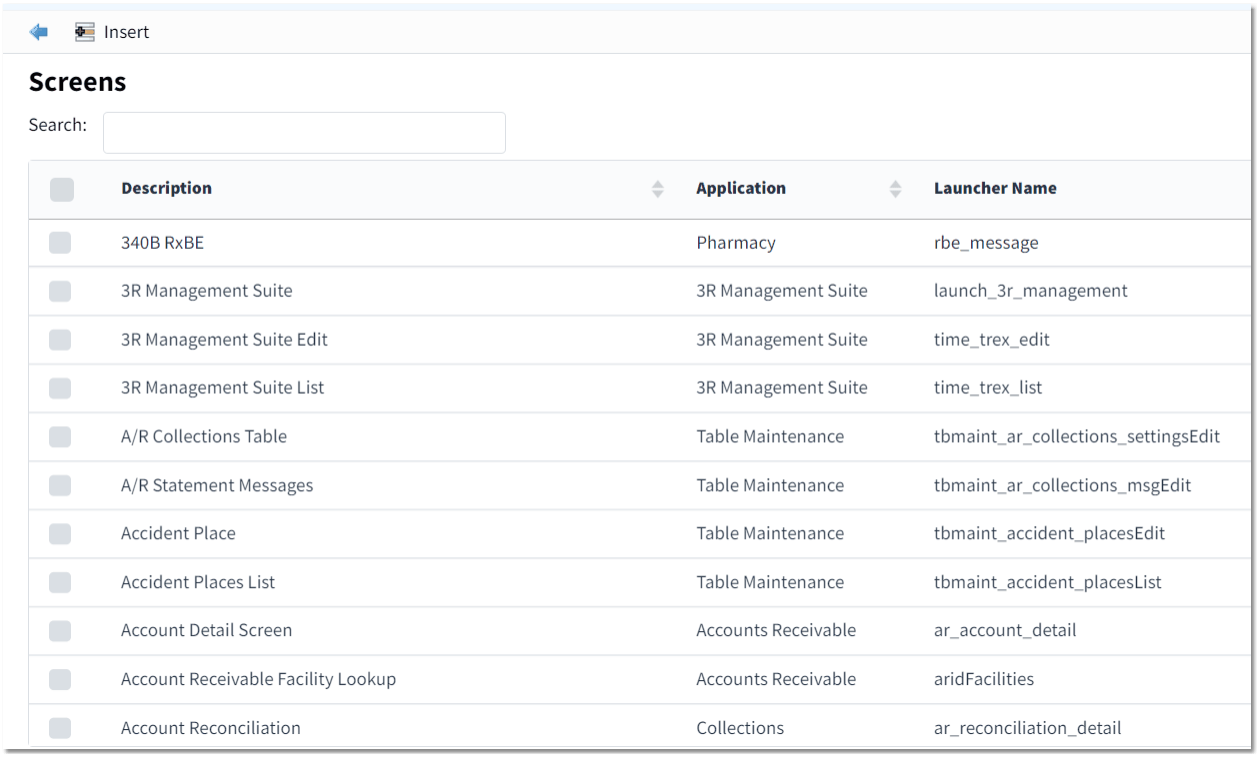
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Screens** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit Screen**



System Administration - Screens

Selecting the word "**Screen"** in **Step 3**, will display any screens that may already exist for the rule. To add a screen, select **Add** from the action bar. To remove a screen from the rule, select the screen so that it is highlighted in blue, then select **Remove** from the action bar.

Select **Web Client > System Administration > Logins > Select Login > Screens > New > Select Condition(s) > Select Action(s) > Edit Screen > Add**



System Administration - Screens

If **Add** is selected, a list will display all available screens. It will show the Description of the screen, the Application in which it is located, and the Launcher Name. Select the screen(s) that the rule is for, then select **Insert** from the action bar.

NOTE: *The Launcher Name is how programs define the screen name.*

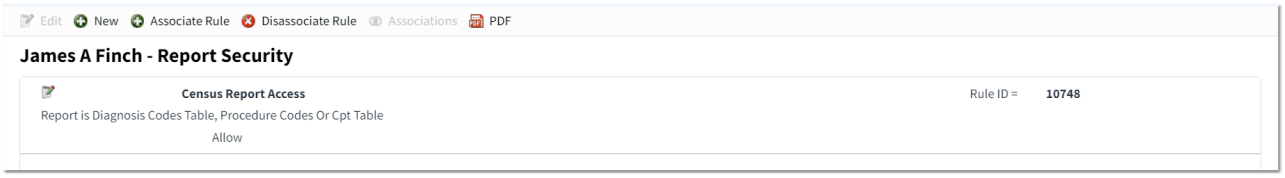
Once **Insert** is selected, the system will go back to the Selected Screens screen. To go back to the rule builder screen, select the **back arrow** from the action bar.

5.7 Reports

Reports rules define which reports a user may access. Report rules only apply to reports using a Report Writer template (reports available on the Report Dashboard).

When **Report** is selected, any rules that have already been set up will display.

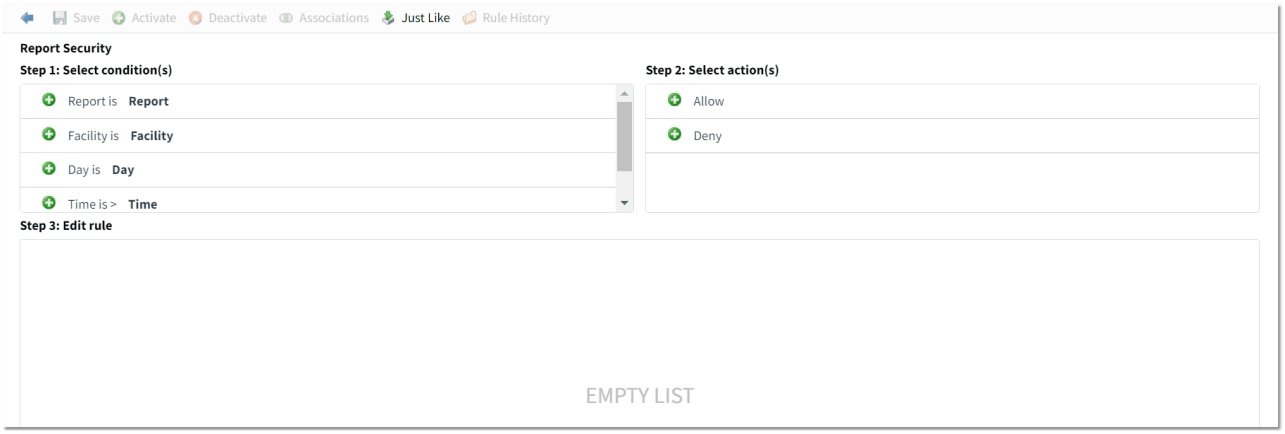
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Report**



System Administration - Reports

To set up a new rule for Reports, select **New** from the action bar. Or select an existing rule and select **Edit**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Reports** > **New**

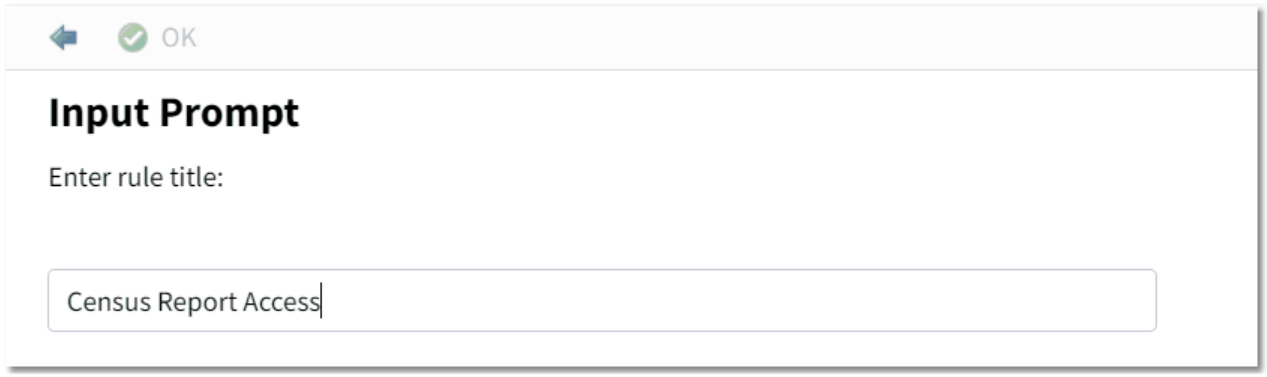


System Administration - Reports

The rule builder screen will then display. Each rule must have a Title. To assign a title to the rule, select the text "**Report Security**." Enter the rule title, then select **Ok**.

***NOTE**: If a rule title is not entered when the rule is saved, the user will be prompted to enter a title. A title must be entered before the rule may be saved.*

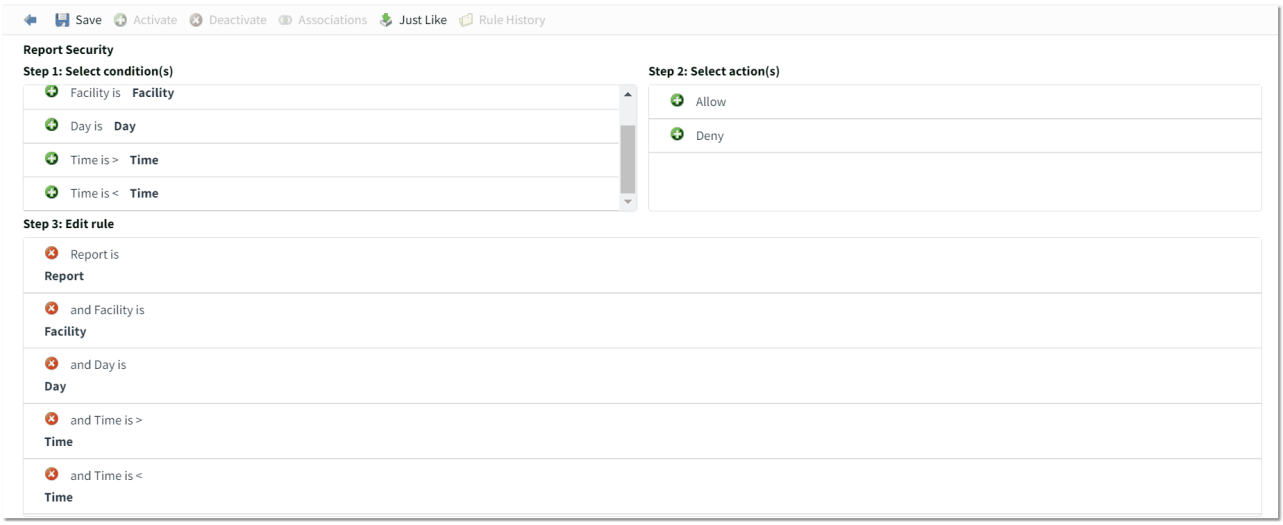
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Reports** > **New** > **Report Security**



System Administration - Reports

In **Step 1**, select the conditions for the rule. The possible conditions include: the Reports that may be accessed, the facilities that may be accessed, the days of the week in which access will be allowed, and an allowable time range for access. For more information on setting up conditions please see Facility 36, Day 37, Start Time 38, End Time 38.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Reports** > **New**

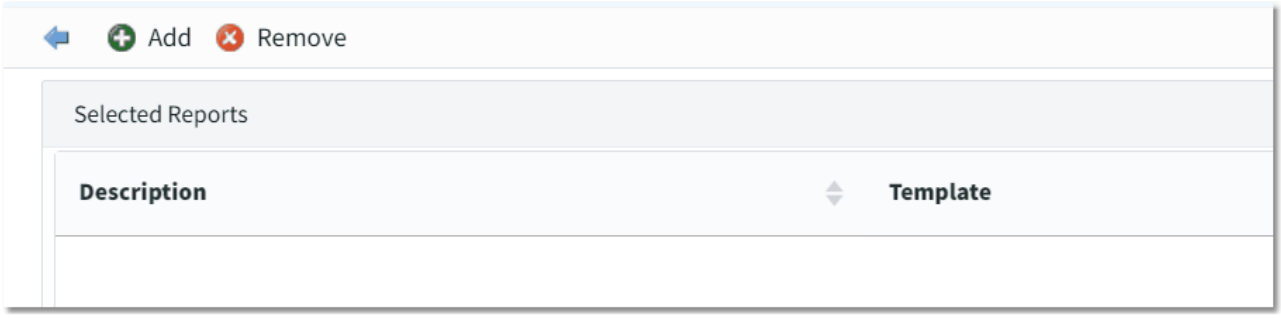


System Administration - Report

In **Step 2**, select the action for the rule. Select the **green plus sign** next to Allow user access or Deny user access.

Once a condition and action have been selected, the rule may be edited in **Step 3**. To do this, select the words in bold lettering (i.e. Report, Facility, Day(s), Start Time, End Time.)

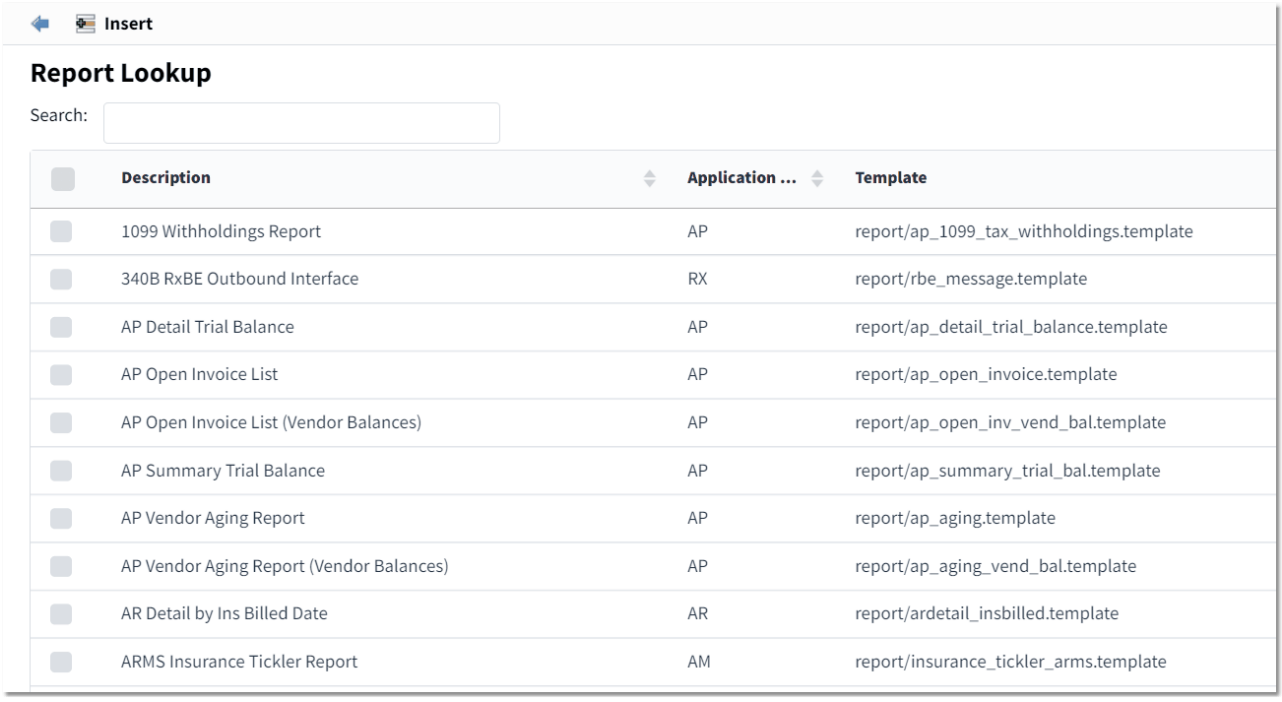
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Reports** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit Report**



System Administration - Reports

Selecting the word "**Report**", in Step 3, will display the reports that have already been selected. If a rule already exists, it may be modified by selecting it from the screen. To add a report, select **Add** from the action bar. To remove a report from this screen, select the report so that it is highlighted in blue, and then select **Remove** from the action bar.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Reports** > **New** > **Select Condition(s)** > **Select Action(s)** > **Edit Report** > **Add**



System Administration - Reports

If **Add** is selected, select the appropriate report(s) that should be added, so it is highlighted in blue, then select **Insert** from the action bar.

Once **Insert** is selected, the system will go back to the Selected Reports screen. To go back to the rule builder screen, select the **back arrow** from the action bar.

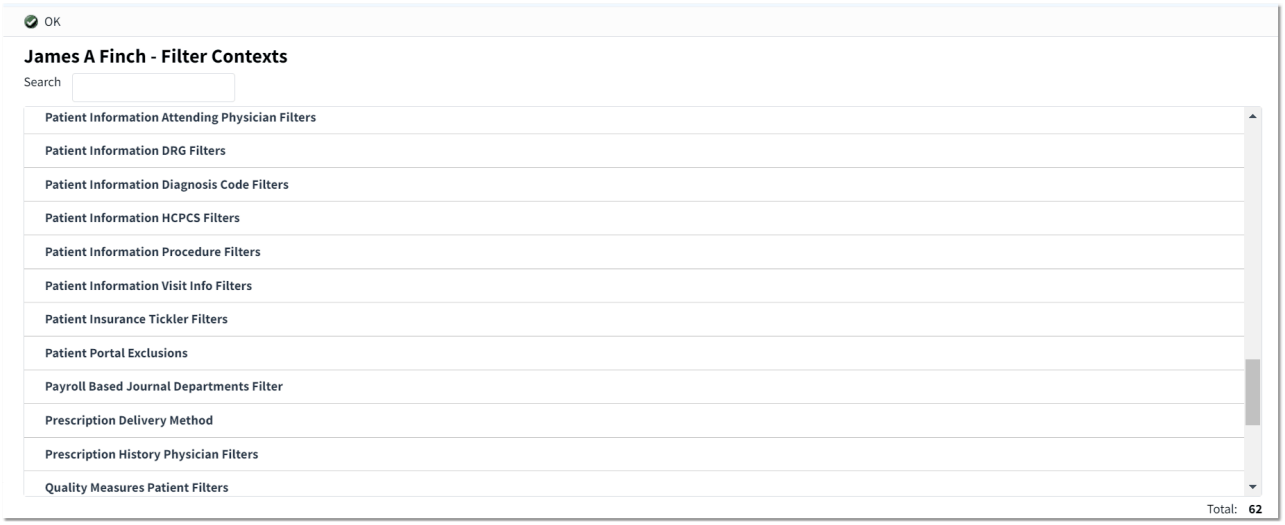
5.8 Custom Reports

This feature is used with the Data Mining application. Please see the Data Mining user guide for more information.

5.9 Filters

The Filters option allows System Administrators to create new filters or edit existing filters and add them to individual logins or roles. When **Filters** is selected, the Filter Contexts screen will display. The Context defines where the filter will be used in the system.

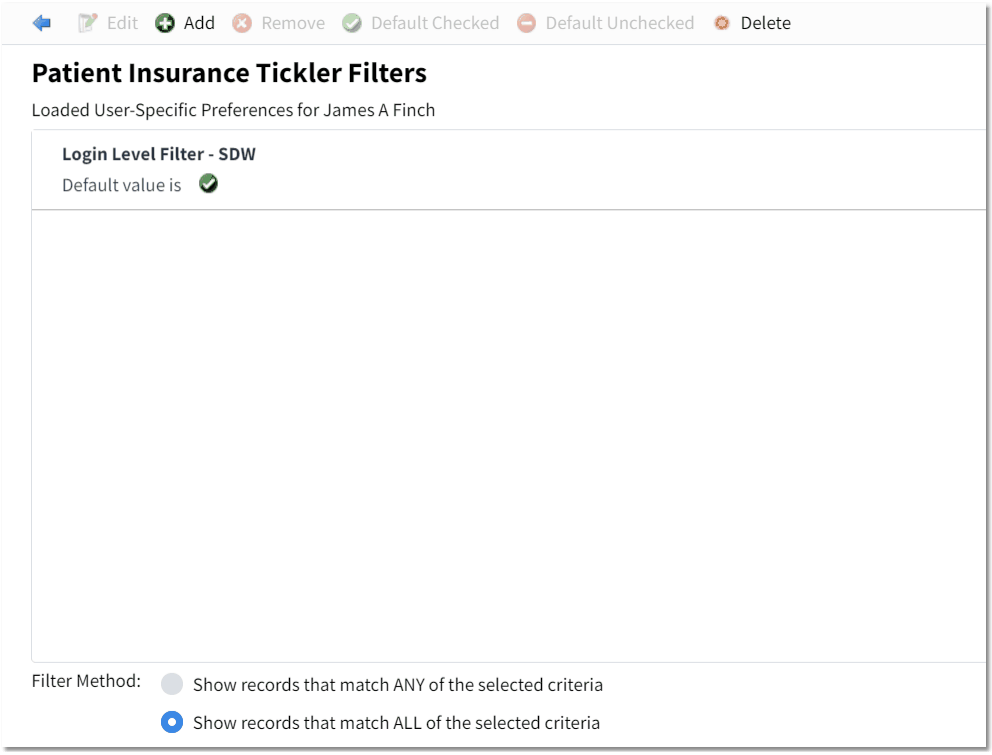
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Filters**



Filter Contexts

After the Context is selected, the Filter Preferences screen will display for the login or role. From here filters used by login or role may be added, removed, or edited.

Select **Web Client > System Administration > Logins > Select Login > Filters > Select Filter Context**



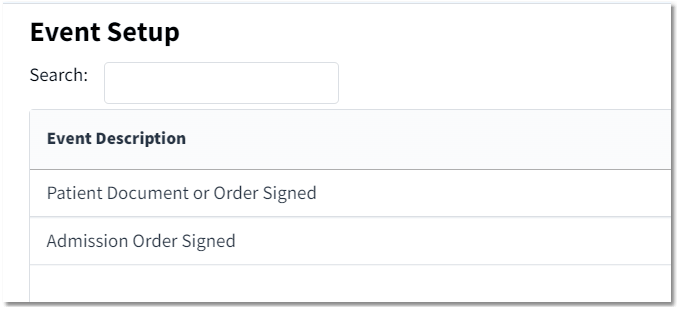
Filter Preferences

For more information on maintaining filters, please see the Filter Builder documentation.

5.10 Events

Events rules may be established to allow actions to occur when an event happens. For example: When a document is e-signed, an action may occur requiring the user have a co-signature.

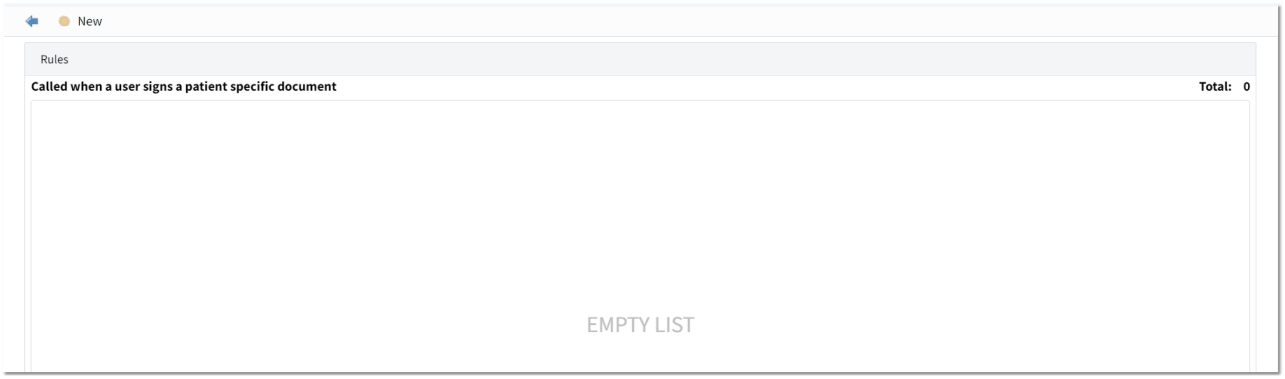
Select **Web Client > System Administration > Logins > Select Login > Events**



System Administration - Events

Select the event to view any rules already set up.

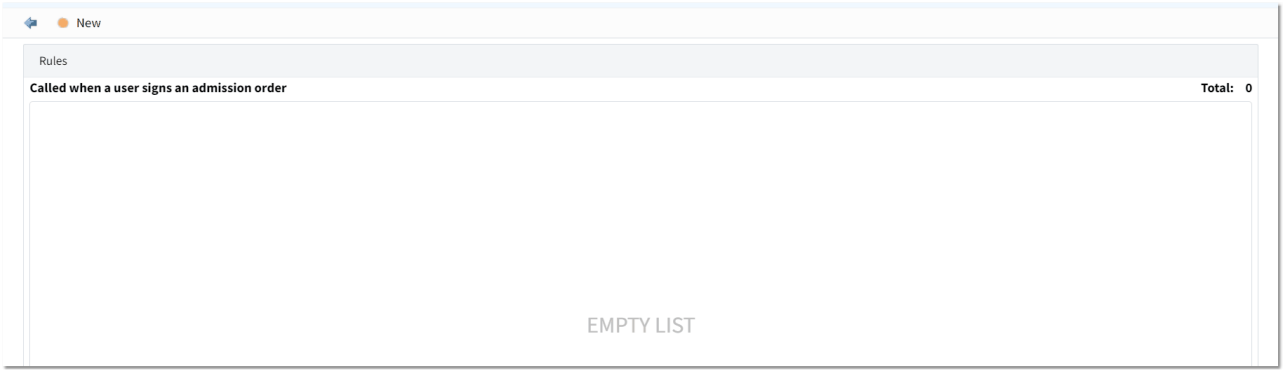
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Events** > **Select Patient Document or Order Signed**



Patient Document Signed

Patient Document or Order Signed will allow a default cosigner(s) to be assigned to a midlevel provider that requires a cosignature on all orders and documents from Physician Documentation and Documentation.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Events** > **Select Admission Order Signed**



Admission Order Signed

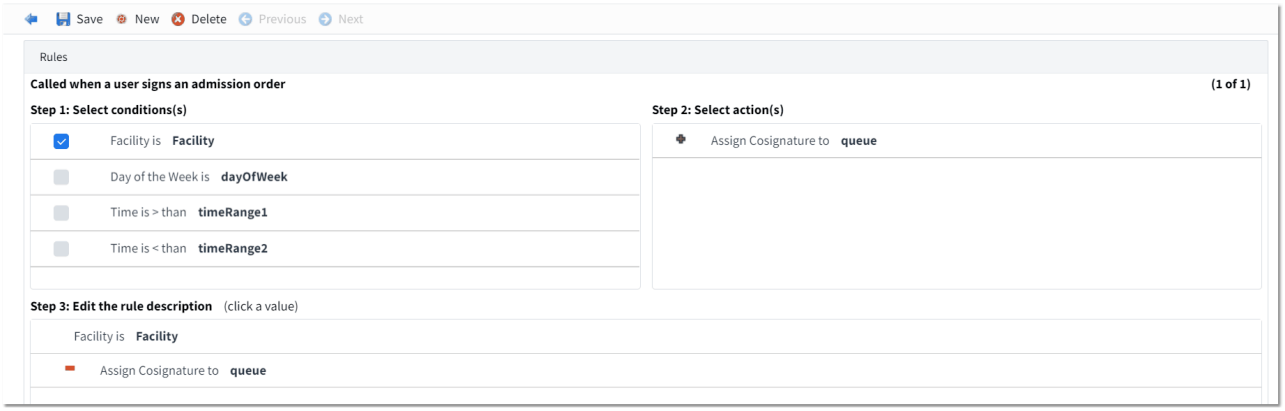
Admission Order Signed will default to None and No Roles. If it is set to Allow and attached to a physician login, the provider would be required to add a cosigner if any admission orders are placed on an ED patient. Non-Admission Orders on an ED patient, or orders placed on non-ED patients, will not prompt/require the user for a cosignature.

If a rule already exists, it may be modified by selecting it from the screen. The screen will be blank if no rules have been set up for the application.

To set up a new rule, select **New** from the action bar.

NOTE: *The user setting this behavior must be assigned to the System Administrator role in order to have permission to assign new Events.*

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Events** > **Select Event** > **New**



System Administration - Events

The rule builder screen will then display. In **Step 1**, select the conditions for the rule. The possible conditions include: the facilities the event applies to, the days of the week in which the event applies and an allowable time range for the event to occur.

In **Step 2**, select the action for the rule. Select the **green plus sign** next to Assign Cosignature to queue for each user, to grant access to the event.

NOTE: *Depending on the event, there may be only one option available in this step.*

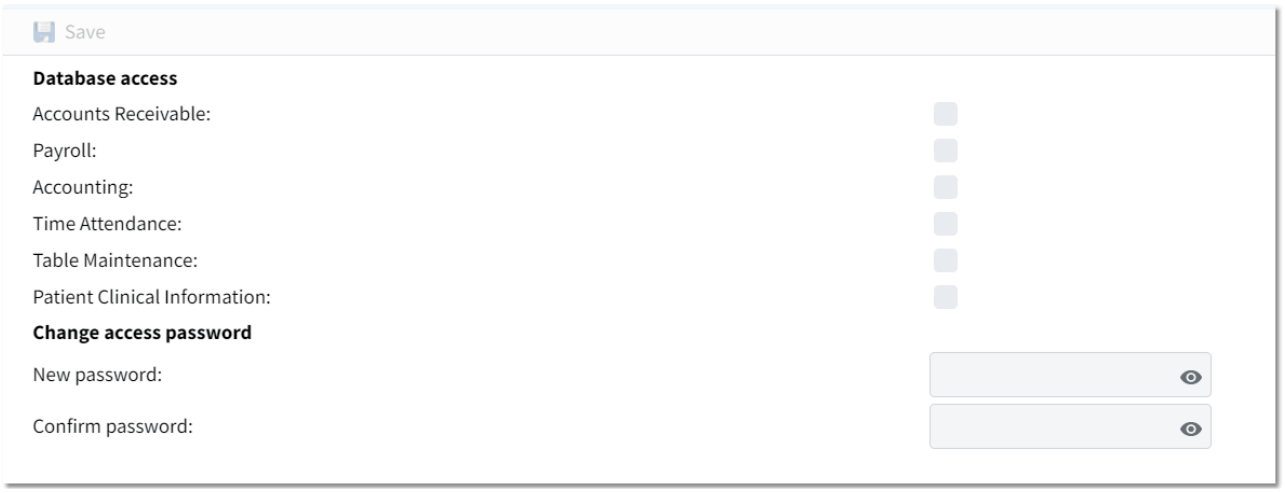
Once a condition and action have been selected, the rule may be edited in **Step 3**. To do this, select the words in bold lettering (i.e. Facility, dayOfWeek, timeRange1, timeRange2.)

NOTE: *To set up the Facility, Day, Start Time and End Time, refer to the* *Facility* 36, *Day* 37, *Start Time* 38, *and End Time* 38 *sections.*

5.11 Database Access

Database Access is used with the Postgres Database application. This is a purchased application that allows direct access to the database where TruBridge stores hospital data, allowing custom reports to be created for each facility.

Select **Web Client** > **System Administraction** > **Logins** > **Select Login** > **Database Access**



Database Access

The password fields are set the user's password to access the database. A password must be set to allow access to the database and must be a minimum of six characters in length.

Select **Save** to save changes.

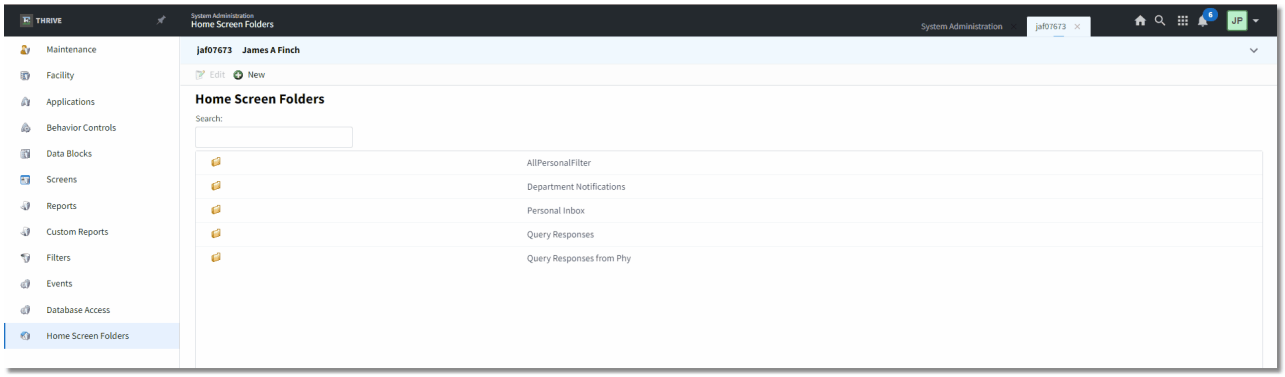
NOTE: *Granting Database Access to a login must be performed by a user in the System Administrator Role, and* ***Allow Database Access*** *must be activated on the user's login Maintenance tab. This option will only be available if ODBC has been purchased. Please contact TruBridge for more information on using this option.*

5.12 Home Screen Folders

The Home Screen Folders option allows system administrators to create new or edit existing folders on a user's Home Screen.

When **Home Screen Folders** is selected, all folders that have been created for the user will display.

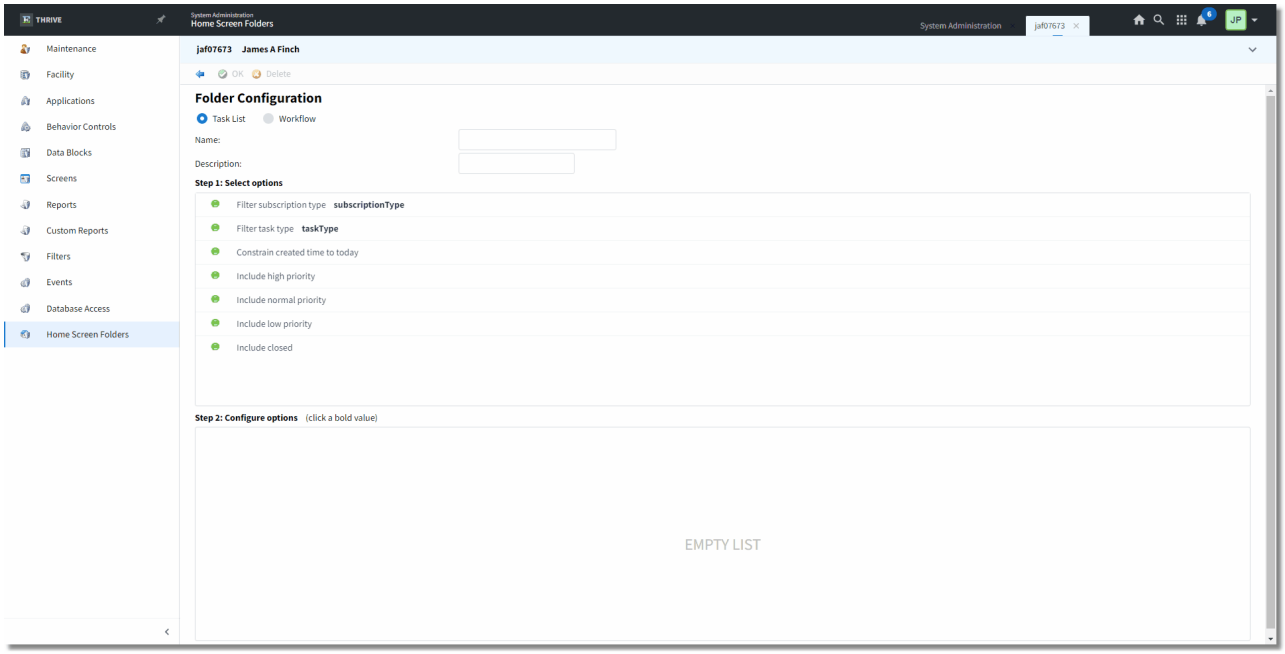
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Home Screen Folders**



Home Screen Folders

To set up a new Folder, select **New** from the action bar or select an existing folder and select **Edit**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Home Screen Folders** > **New**



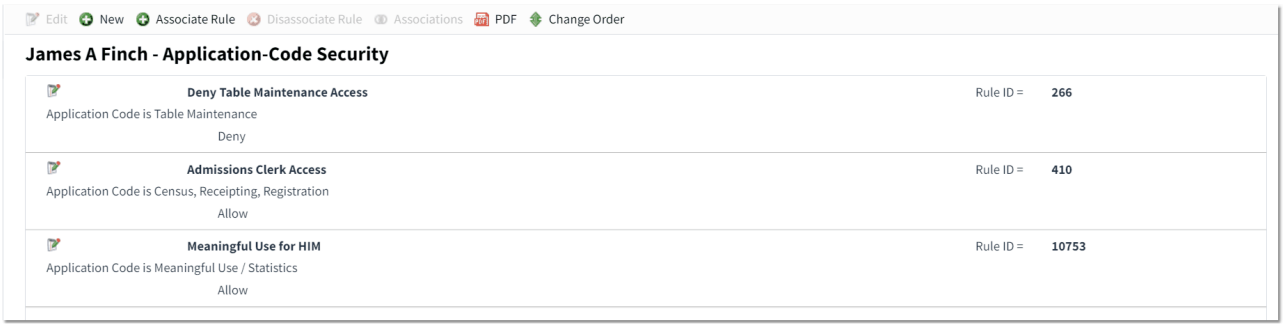
Home Screen Folder - New

The Folder Configuration screen will need to be completed to set up the folder. For Information on creating new folders please see the Home Screen user guide.

5.13 Action Bar Options

Each of the options on the action bar assists in creating and editing rules as well as reporting for rules for each user login or role.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control**



System Administration - Action Bar Options

Below is an explanation of each option:

- **Edit:** Select this option to make any changes to an existing rule.
- **New:** Select this option to create a new rule.
- **Associate Rule:** Select this option associate a single rule with multiple logins. When selected, a list will display all of the rules that have already been set up for any user login or role. Once the rule has been selected, the rule is attached to the user login or role. For example, if login A has security for Accounts Payable, then go to login B, and use the Associate Rule feature to add the same rule to login B.
  - When this option is used for more than one user login, the exact same rule will be used for all attached user logins. For examples if login A and B are using the same rule, if a change is made to that rule on either user login, both logins will be affected. For more information on how this option is used, please see the Associate Rule 59 section of this user guide.
- **Disassociate Rule**: Select this option to remove the user from the rule.
- **Associations:** Selecting this option will display all user logins or roles using the selected rule. If the same rule is attached to more than one user login, it is important to be able to see what user logins are using the rule in the case changes need to be made to the rule.

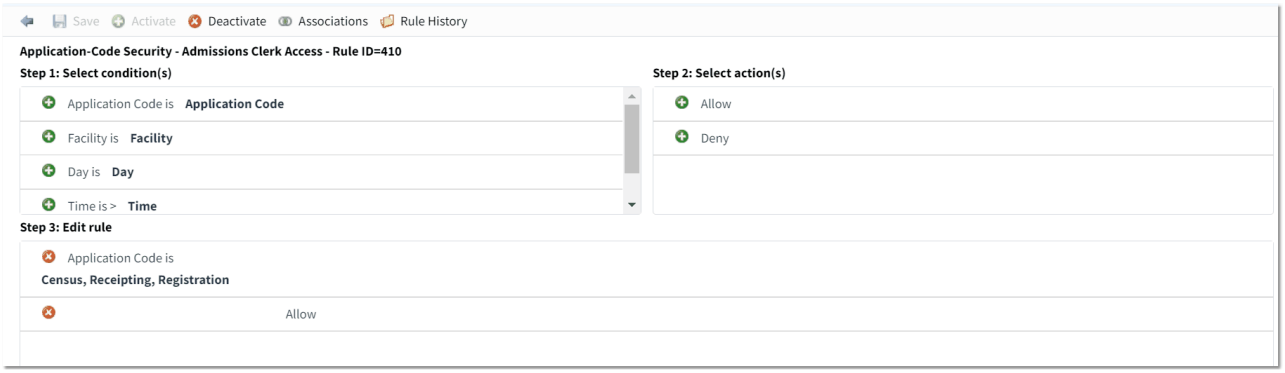
- **PDF:** Selecting this option gives the ability to put the information displayed on the screen in a PDF report format. For example, this option may be used to print a list of all user logins with access to the Pharmacy application or a list of user logins attached to the Employee Roles group.

- **Change Order:** This option will only appear if there are multiple rules set up. It will allow the order of the rules to be changed. With the ability to share rules among a group of users, there will be times when a specific rule will need to be shared but also be able to deny one specific aspect of the shared rule for a specific user. Example: There is a screen rule set up for a group of users who need access to the Item Master. The rule has the following screens set to Allow:
  - Item Master
  - Item Master (edit)
  - Item Master CPT Edit
  - Item Master Order Entry
  - Item Master Pharmacy
  - Item Master Pricing

In this group, there are three users who DO NOT need access to Item Master Pricing. The users still need the shared rule in case changes or additions are made to the rule at a later time. This is so all three employees do not have to be edited individually. The employees would then be given access to the shared rule, but an additional rule will need to be created to deny access to Item Master Pricing on the three employees who do not need the screen. The deny access rule would need to be listed ABOVE the shared rule. For this reason, it is recommended that any deny rules be moved to the top of the rule list. For more information on how this option is used, please see the Change Order 60 section of this user guide.

Rule Maintenance

Select **Web Client > System Administration > Logins > Select Login > Application, Screen, Report, or Behavior Control > Select Rule > Edit**



System Administration - Action Bar Options

Below is an explanation of each option:

- **Save:** Selecting this option to save any changes made to the rule.

- **Activate**: Selecting this option activates a rule previously deactivated. See Activate 61 for more details.

- **Deactivate**: Selecting this option will disassociate the rule from ALL users and mark the rule as Inactive. The rule may later be re-activated by selecting the Activate option. See Deactivate 62 for more details.

- **Associations:** Selecting this option will display all user logins or roles using the selected rule. If the same rule is attached to more than one user login, it is important to be able to see what user logins are using the rule in the case changes need to be made to the rule.

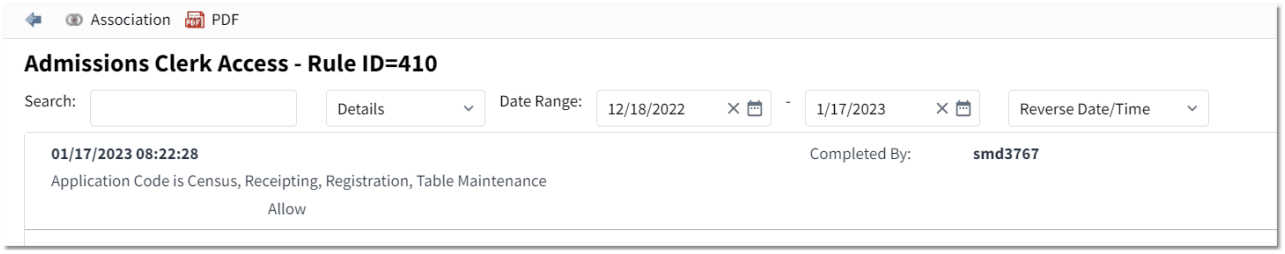
- **Just Like:** This option is only available when creating a New rule.Selecting this option will allow the rule to be copied and then saved. The difference between this option and the Add option is this one creates a new rule not associated with the rule it is being copied from. For example, there is an existing rule with access to the Census and Coding applications. Login A is needing this rule but also needs access to the E-forms application. A new rule may first be selected and then Just Like may be used to copy over the information where changes may be made. Once Save is selected, the rule will then need to be given a title. For more information on how this option is used, please see the Just Like Option 63 section of this user guide.

- **Rule History**: Provides a listing of changes made to the rule. See below for details.

Rule History

Once Rule History is selected, a list of changes made to the rule will display. When a change is made to a rule, the updated version of the rule will be displayed at the top of the rule history list. Thrive will continue to track any additional changes made to the rule. The list will display the newest version of the rule at the top of the screen and the oldest version at the bottom of the screen. Search tools are available to help identify specific changes.

Select **Web Client > System Administration > Logins > Select Login > Application, Screen, Report, or Behavior Control > Select Rule > Edit > Rule History**



Rule History

The following information displays on the screen:

- **Date/Time**: The date/time that the change was made to the rule.

- **Rule Details**: Shows the application, screen, report, or behavior controls either allowed or denied by the rule.
- **Completed By**: The login that made the change to the rule.

Rule History is also available at the system level. See Rule History 104 for more information.

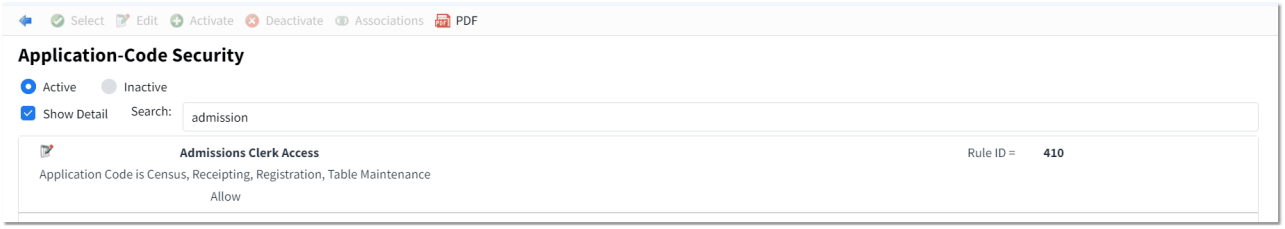
Associate Rule

This section demonstrates how to use the Associate Rule option on the action bar when a login or role is accessed. The Associate Rule option is also available from Rule Management. In Rule Management, rules may be associated to multiple logins and/or roles at one time.

Once a user login or role has been selected, select **Associate Rule** from the action bar.

A list of all existing rules will display. A search feature is available to search for rules by title, or code (Application Code, Screen Code, Report Code, Behavior Control Code). Options are available to filter the search results for just Active or Inactive rules. If an inactive rule is selected, it must be activated prior to adding it to a login. Select the appropriate rule needing to be added to the user login or role so it is highlighted in blue. Then choose **Select** from the action bar.

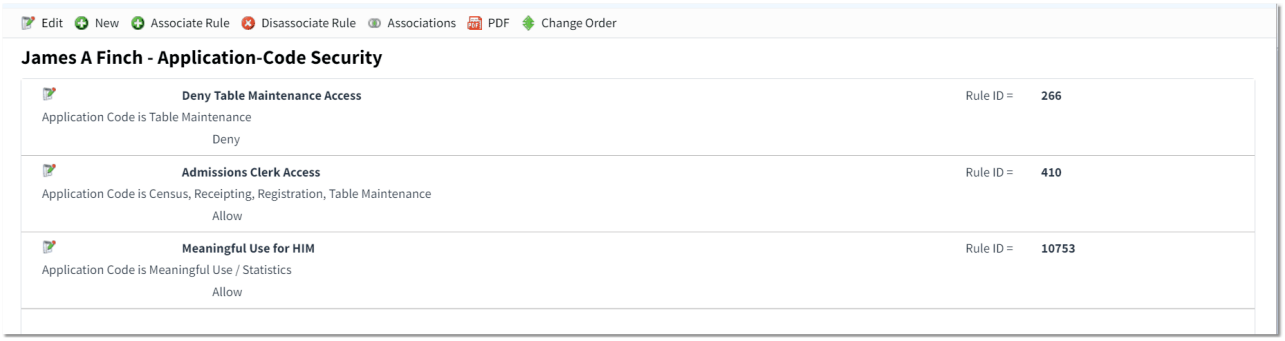
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control** > **Associate Rule**



System Administration - Associate Rule

The rule will then be added and applied to the selected user login or role.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control**



System Administration - Associate Rule

NOTE: *This option is only available for Applications, Screens, Reports, Behavior Controls, Data Block, and Custom Report rules.*

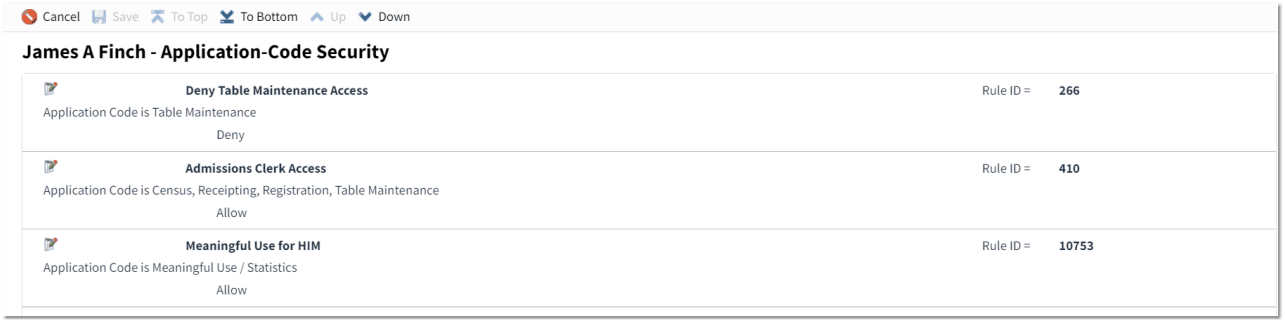
Change Order

This demonstrates how to use the Change Order option on the action bar.

Once a user login or role has been selected, select **Change Order** from the action bar.

A list of options will appear on the action bar. Select the rule to move it either to the top or bottom, or select if it needs to be moved up or down to be in a specific order. Once the rules are in the appropriate order, select **Save**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control** > **Change Order**



System Administration - Change Order

Activate

An inactive rule may not be Associated with a login. Instead, these rules must be reactivated prior to being added to a login.

To do this, select **Associate Rule** to display a list of all existing rules.

Select the **Inactive** option to display the rules that have been deactivated.

Search for the desired rule, select the rule, then select **Activate**.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control** > **Associate Rule**

Activate Rules

The rule will now be active. Select **Active** and search for the desired rule, select the rule, and choose **Select** to continue with Associate Rule 59. Inactive rules may also be activated from Rule Management.

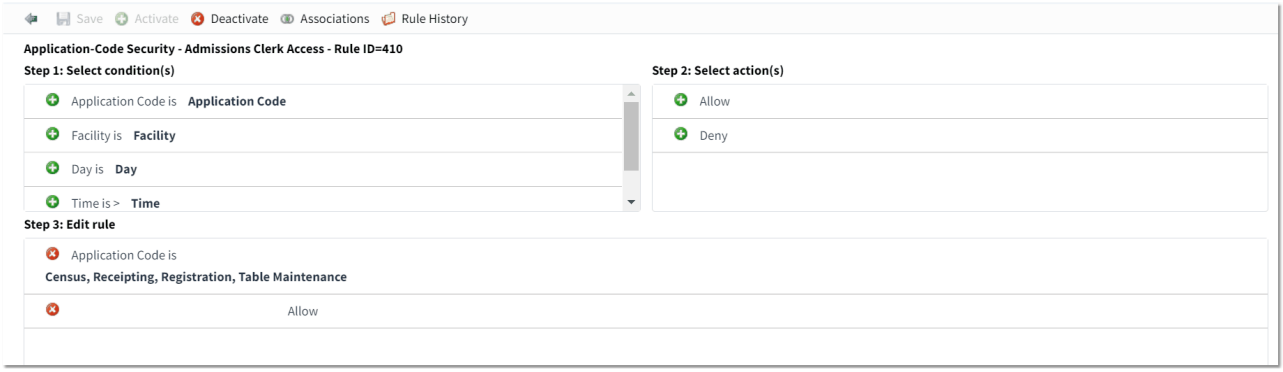
Deactivate

When a rule is deactivated, it will be removed from all associated logins.

To deactivate a rule, select the rule then select **Edit**.

From the rule edit screen, select **Deactivate**.

Select **Web Client > System Administration > Logins > Select Login > Application, Screen, Report, or Behavior Control > Select Rule > Edit**



Deactivate Rule

A prompt will display indicating the number of entities (logins/roles) the rule is associated with; select **Yes** to deactivate the rule or select **No** to keep the rule active.

Select **System Administration > Logins > Select Login > Application, Screen, Report, or Behavior Control > Select Rule > Edit > Deactivate**

Deactivate Rule

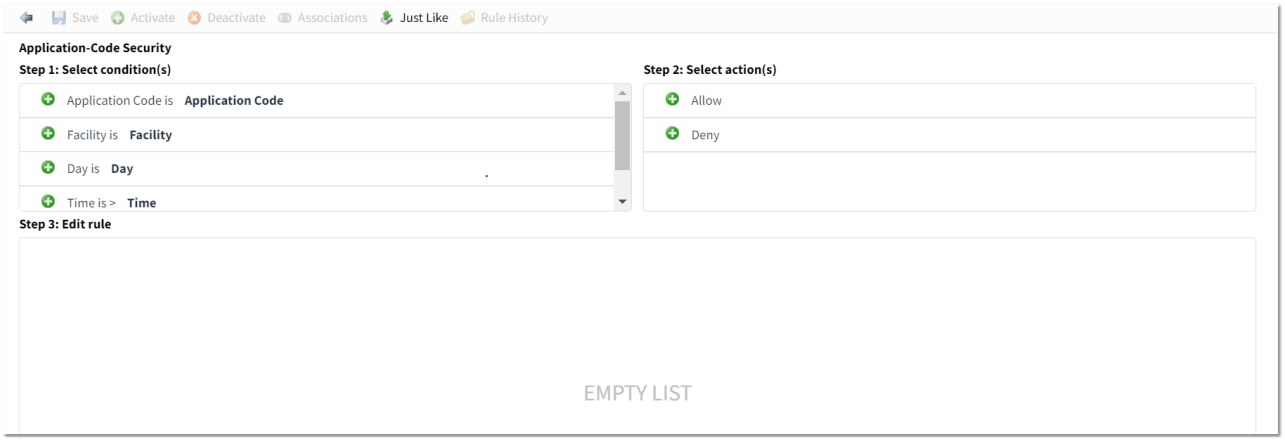
Rules may also be Deactivated from Rule Management.

Just Like Option

This section demonstrates how to use the Just Like option in the rule maintenance screen.

Once a user login or role has been selected, select **New** from the action bar.

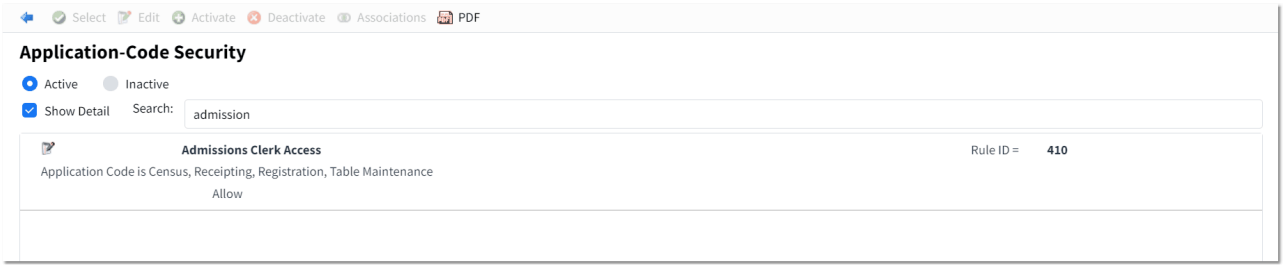
Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control** > **New**



System Administration - Just Like Option

Select **Just Like** from the action bar. A list of existing rules will display. Select the appropriate rule that needs to be just liked to the user login or role so it is highlighted in blue. Then choose **Select** from the action bar.

Select **Web Client** > **System Administration** > **Logins** > **Select Login** > **Application, Screen, Report, or Behavior Control** > **New** > **Just Like**



System Administration - Just Like Option

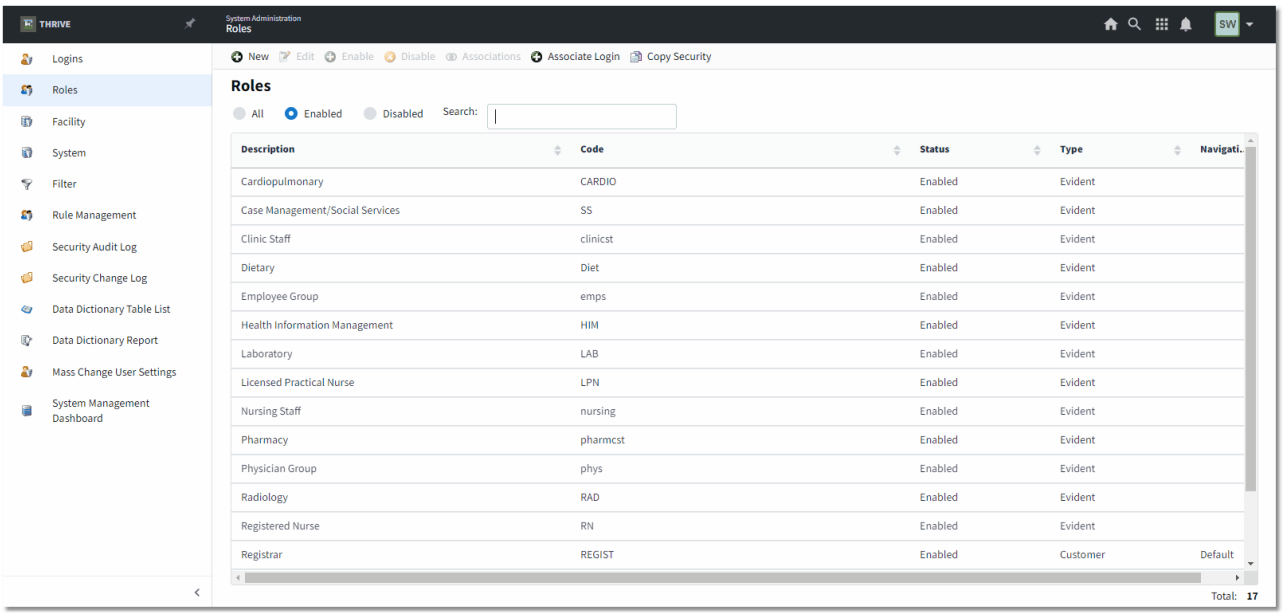
Make any necessary changes to the rule and then select **Save** from the action bar.

The system will then prompt for a new rule title to be entered. After the title has been entered, select **OK** from the action bar.

The Just Like option is available when creating rules from Rule Management.

Chapter 6 Roles

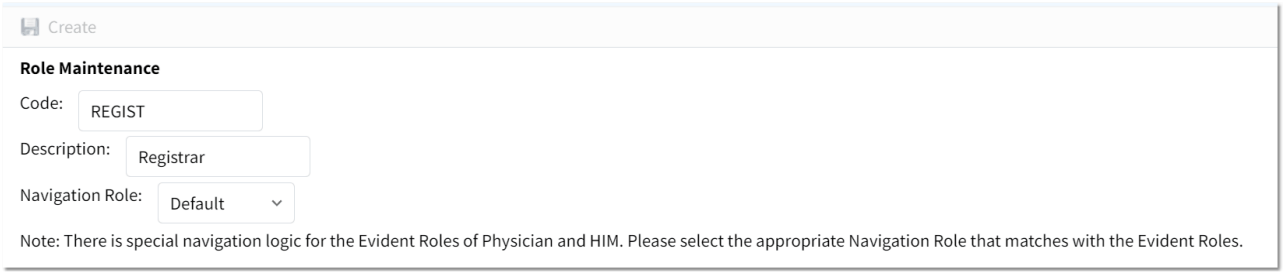
Select **Web Client** > **System Administration** > **Roles**



System Administration - Roles

After selecting **Roles**, the existing roles will display. A set of TruBridge defined roles will be available. All TruBridge roles will display with TruBridge in the Type column. These TruBridge roles also have default security rules attached to them. Custom roles may be created by selecting **New** to create a new role.

Select **Web Client** > **System Administration** > **Roles**



System Administration - New Role

Complete the following information:

- **Code**: A unique code is assigned to each role. Enter any code up to eight characters in length.
- **Description**: Enter the name of the role.

- **Navigation Role**: There is special navigation logic for the TruBridge Default Roles of Physician and Health Information Management (HIM). To ensure the custom role will have the desired navigational features, select the related role.
  - **Default**: Used for roles that will not be associated with Physician or HIM logins. (ex. Nursing and other hospital staff)
  - **Physician**: Used for roles that will be associated with Physician logins.
  - **HIM**: Used for roles that will be associated with HIM logins.

Once all information has been completed, select **Create**.

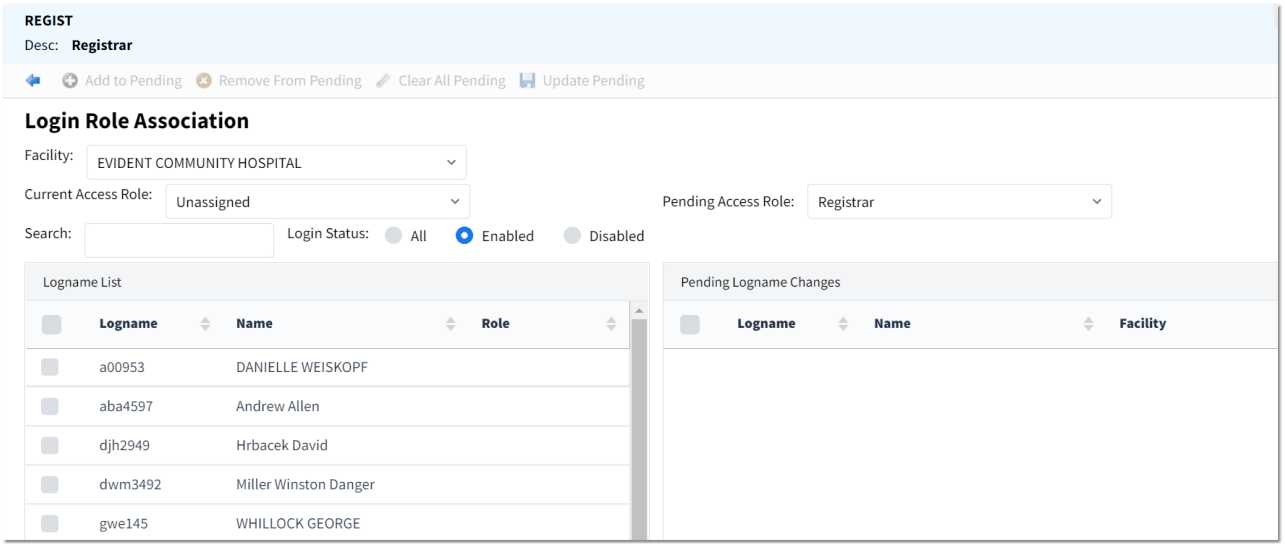
Security rules may be setup on a role. This allows security to be addressed for a group of logins that share the same role, rather than individually on each login. Every login will be assigned to a role. Roles may be assigned to a login using the Associate Login option on the action bar or by accessing the login from the Logins screen and updating it on the Facility tab. The Associate Login option is discussed below. For information on assigning roles from the Login screen, please see the Facility 21 documentation located under the Logins section.

NOTE: *Logins may only have one role.*

Associate Login

The Associate Login option may be used to assign logins to a role. To begin, from the Role Edit screen, or from the Roles screen, select **Associate Login**.

Select **Web Client** > **System Administration** > **Roles** > **Select a Role** > **Associate Login**



Roles - Associate Logins

Double-click the logins that should be assigned to the role from the Logname List. Search tools are available to filter the list by Facility and Current Access Role. Specific logins may be found using the search bar. Once a login is selected, it will display in the Pending Logname Changes list. Select **Update Pending** to replace the user's current role, with the new role.

***NOTE**: For existing roles, the Associate Login option is also accessible from the Roles screen.*

Security rules may be added to a role using the Copy Security option or Rule Management. The Copy Security option is discussed below. For information on assigning rules using Rule Management, please refer to the Rule Management 102 section.

Copy Security

The Copy Security option may be used to copy security rules from one role to another.

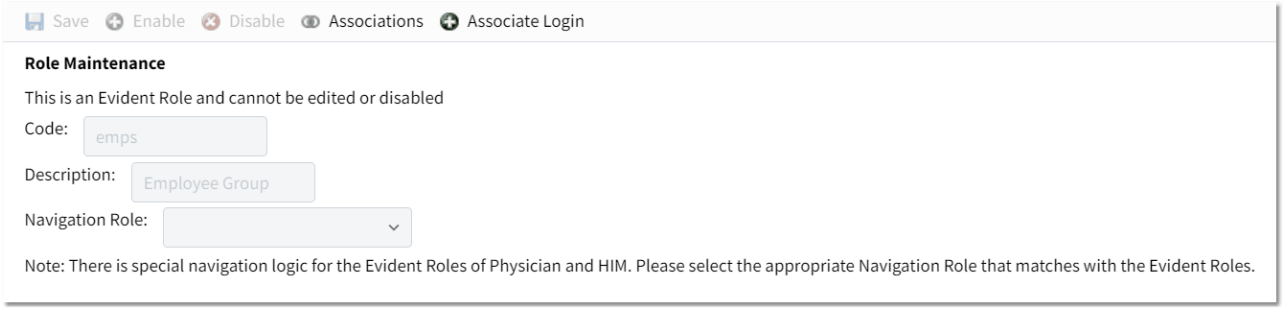
To begin, from the Roles screen, select the role to copy security to, then select **Copy Security**.

Next, select the role to copy security from, then select **Ok**. The system will prompt for the types of rules to be copied; select **All** or select specific types of rules to copy, then select **Copy**. A warning will display if rules already exist on the role that security is being copied to. Proceeding with copying will overwrite the existing rules with the rule being copied.

6.1 Maintenance

Once one of the roles is selected, the Role Name and Description will display. Custom roles will also display the Navigation Role. Different options for setting up rules will display on the navigation bar.

Select **Web Client** > **System Administration** > **Roles** > **Select Role**

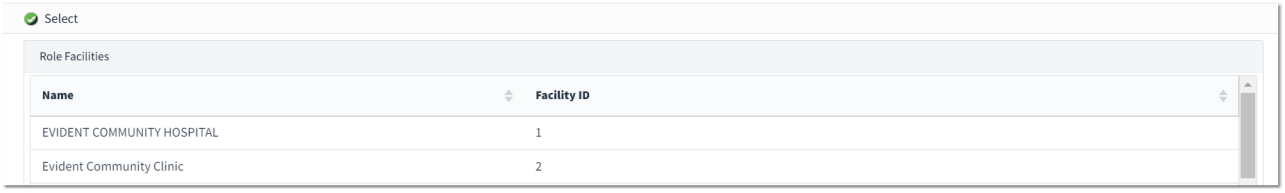


System Administration - Maintenance

6.2 Facility

When **Facility** is selected, a list of available facilities will display.

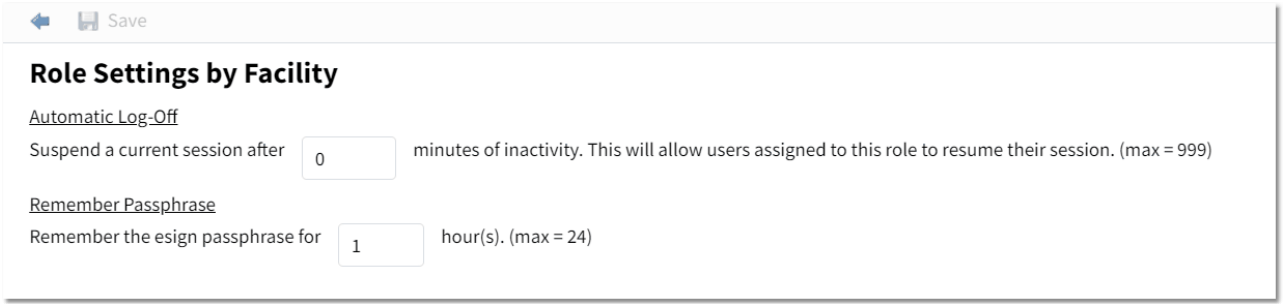
Select **Web Client** > **System Administration** > **Roles** > **Select Role** > **Select Facility**



Role Facilities

Once a facility is chosen, inactivity settings and remember passphrase hours may be established for all users who are assigned to the role at that facility.

Select **Web Client** > **System Administration** > **Roles** > **Select Role** > **Select Facility** > **Choose a Facility**



Role Settings by Facility

- **Automatic Log-Off**: Enter the number of minutes of inactivity to be reached before a user is suspended from a current session. Once logged off, the user must enter the password for the login to resume the session. The maximum setting is 999 minutes. This setting will override the global inactivity timeout settings located on the System screen in System Administration. Select **Save** to keep any changes.

- **Remember Passphrase**: Enter the number of hours the system should remember the passphrase for the role. The maximum is 24 hours.
  - The **Remember Passphrase** behavior will default to one hour.
  - If the role or user has **Remember Passphrase,** Thrive will read the login's facility setting first.
  - If the login's facility setting is blank, Thrive will read the role's **Remember Passphrase** facility setting.

6.3 Application Defaults

The following are application access defaults for each role. No changes may be made to these default settings. If an additional application needs to be given to a role, a new rule will need to be set up allowing access. If one of the default settings needs to be denied, a new rule will need to be set up denying access. See the Application 92 section for more information on application access and instructions on how to add or remove application access for a specific role.

- Cardiopulmonary Role Application Defaults:
  - Clinical Information
  - Order Entry
  - Home Screen
  - Medication Reconciliation
  - Report Writer
  - Resulting
  - Rule Builder
  - E-forms
  - Health History
  - MAR
  - System Utility
  - Help
  - Thrive UX
  - Medical Necessity
  - Documentation
  - Communication
  - Problem List
  - Census
  - Table Maintenance

- Case Management/Social Service Role Application Defaults:
  - Electronic Signature
  - EMR Viewer
  - Home Screen
  - Medication Reconciliation
  - Order Entry
  - Prescription Writer
  - Problem List
  - Report Writer
  - Rule Builder
  - Health History
  - MAR
  - System Utility
  - Help
  - Thrive UX
  - Medical Necessity
  - Patient Education
  - Communication
  - Implantable Devices
  - Census
  - Table Maintenance

- Clinic Staff
  - Home Screen
  - Enterprise Wide Scheduling
  - Medical Practice
  - Report Writer
  - System Utility
  - Patient Education
  - Help
  - Thrive UX
  - Communication
  - Medical Necessity
  - Census
  - Table Maintenance

- Dietary Role Application Defaults:
  - Home Screen
  - Report Writer
  - Order Entry
  - Rule Builder
  - Clinical Information
  - System Utility
  - Help
  - Thrive UX
  - Communication
  - Medical Necessity
  - Table Maintenance

- Employee Role Application Defaults:
  - Report Writer
  - Rule Builder
  - Home Screen
  - Electronic Signature
  - System Utility
  - Help
  - Thrive UX
  - Communication
  - Medical Necessity
  - Table Maintenance

- Health Information Management Role Application Defaults:
  - Electronic Signature
  - Home Screen
  - Coding
  - Problem List
  - Report Writer
  - Health Information Management
  - Resulting
  - Rule Builder
  - Health History
  - System Utility
  - Consolidated Clinical Document Architecture
  - Charge Entry

- Help
- Thrive UX
- Clinical Information
- Medical Necessity
- Documentation
- Implantable Devices
- Information Submission
- Communication
- Cancer Registry
- Census
- Table Maintenance

- Laboratory Role Application Defaults:
  - Home Screen
  - Report Writer
  - Order Entry
  - Resulting
  - Rule Builder
  - Clinical Information
  - E-forms
  - System Utility
  - Help
  - Thrive UX
  - Medical Necessity
  - Communication
  - Antimicrobial Reporting
  - Census
  - Table Maintenance

- Licensed Practical Nurse Role Application Defaults:
  - Census
  - Electronic Signature
  - ChartLink
  - Clinical Information
  - E-forms
  - EMR Viewer
  - Home Screen
  - Home Health
  - ImageLink
  - MAR
  - Medication Reconciliation
  - Medication Verification
  - Order Entry
  - Prescription Writer
  - Problem List
  - Report Writer
  - Resulting
  - Rule Builder
  - Health History
  - POC Order Entry
  - System Utility
  - InfoButton

  - Charge Entry
  - Patient Education
  - Help
  - Thrive UX
  - Medical Necessity
  - Implantable Devices
  - Communication
  - Documentation
  - Census
  - Table Maintenance

- Nursing Staff Role Application Defaults:
  - Census
  - ChartLink
  - E-forms
  - EMR Viewer
  - Home Screen
  - Future Order
  - ImageLink
  - MAR
  - Medication Reconciliation
  - Medication Verification
  - Order Entry
  - Clinical Information
  - Report Writer
  - Rule Builder
  - Prescription Writer
  - POC Order Entry
  - System Utility
  - Charge Entry
  - Patient Education
  - Help
  - Thrive UX
  - Medical Necessity
  - Communication
  - Documentation
  - Table Maintenance
  - Communication
  - Problem List

- Pharmacy Role Application Defaults:
  - E-forms
  - Home Screen
  - MAR
  - Medication Reconciliation
  - Order Entry
  - Prescription Writer
  - Problem List
  - Report Writer
  - Clinical Information
  - Rule Builder
  - Health History

- System Utility
- InfoButton
- Help
- Thrive UX
- Pharmacy
- Medical Necessity
- Communication
- Implantable Devices
- Charge Entry
- Table Maintenance
- Census
- Medication Verification
- POC Order Entry
- CPOE

- Physicians Role Application Defaults:
  - ChartLink
  - Clinical Information
  - CPOE
  - E-forms
  - Electronic Signature
  - Health History
  - Home Screen
  - ImageLink
  - MAR
  - Medication Reconciliation
  - Order Entry
  - Phys Doc
  - Prescription Writer
  - Problem List
  - Report Writer
  - Resulting
  - Table Maintenance
  - Rule Builder
  - System Utility
  - Health Information Management
  - Consolidated Clinical Document Architecture
  - Health Information Resource
  - InfoButton
  - Charge Entry
  - Plan of Care
  - Patient Education
  - Help
  - Thrive UX
  - Medical Necessity
  - Documentation
  - Implantable Devices
  - Cancer Registry
  - Communication
  - Clinical Reconciliation
  - Census
  - Secure Messaging

- Radiology Role Application Defaults:
  - Home Screen
  - Order Entry
  - Report Writer
  - Resulting
  - Rule Builder
  - Clinical Information
  - ImageLink
  - System Utility
  - Help
  - Thrive UX
  - Communication
  - Medical Necessity
  - Census
  - Table Maintenance

- Registered Nurse Role Application Defaults:
  - Consolidated Clinical Document Architecture
  - Census
  - ChartLink
  - E-forms
  - EMR Viewer
  - Home Screen
  - Home Health
  - ImageLink
  - MAR
  - Medication Reconciliation
  - Medication Verification
  - Order Entry
  - Clinical Information
  - Prescription Writer
  - Problem List
  - RAI / MDS
  - Report Writer
  - Resulting, Rule Builder
  - Health History
  - POC Order Entry
  - System Utility
  - InfoButton
  - Charge Entry
  - Plan of Care
  - Patient Education
  - Help
  - Thrive UX
  - Medical Necessity
  - Documentation
  - Implantable Devices
  - Antimicrobial Reporting
  - Communication
  - Clinical Reconciliation
  - Census

  - Table Maintenance

- Rehabilitation Services Role Application Defaults:
  - Home Screen
  - Order Entry
  - Report Writer
  - Resulting
  - Rule Builder
  - Clinical Information
  - E-forms
  - Health History
  - System Utility
  - Patient Education
  - Thrive UX
  - Help
  - Medical Necessity
  - Documentation
  - Communication
  - Problem List
  - Census
  - Table Maintenance

- Schedulers Role Application Defaults:
  - Home Screen
  - Report Writer
  - Rule Builder
  - System Utility
  - Help
  - Thrive UX
  - Communication
  - Medical Necessity
  - Enterprise Wide Scheduling
  - ChartLink
  - Census
  - Table Maintenance

- System Administrator Role Application Defaults:
  - Consolidated Clinical Document Architecture
  - Auditing
  - Database Access
  - Data Dictionary
  - Report Writer
  - Rule Builder
  - Security
  - System Management
  - System Utility
  - Table Maintenance
  - Meaningful Use / Statistics
  - Health Information Resource
  - Plan of Care
  - Home Screen
  - Help

- Thrive UX
- Medical Necessity
- Data Export
- Report Scheduler
- Communication
- Census
- Notes

***NOTE**: The TruBridge Default Application Rule for each role will be automatically associated with each role. The rule will be associated at the end of the rule list where all rules above will take precedence over it. A deny rule may be created and inserted above the TruBridge default rule if necessary; this will allow flexibility in denying or allowing resources.*

6.4 Behavior Control Defaults

The following are behavior controls that default to "Allow" for each role. No changes may be made to these default settings. If an additional "allowed" behavior control needs to be added to a role, a new rule will need to be set up which allows access. If one of the default settings needs to be denied, a new rule will need to be set up which denies access. See the Control 39 section for more information on behavior control access and instructions on how to add or remove behavior control access for a specific role.

- Cardiopulmonary Default Behavior Controls
  - Prompt for Medical Necessity Check
  - Review Medical Necessity
  - User is allowed to document
  - Edit Working Diagnosis
  - Administer Medications
  - Ablility to edit Receive Information on Hospital Ancillary Orders
  - Collect/Receive Ancillary Orders
  - Access to System Menu
  - Access Learning Management System

- Case Management/Social Services Default Behavior Controls
    - Access Learning Management System
  - Thrive UX System Menu

- Clinic Staff Default Behavior Controls
  - Access to System Menu
  - Edit Consent/Privacy Notice
  - Edit Med History Consent
  - Access Learning Management System
  - Chief Complaint Read Only
  - Problems Read Only
  - Surgery Read Only

- Dietary Default Behavior Controls
  - Ablility to edit Receive Information on Hospital Ancillary Orders
  - Collect/Receive Ancillary Orders
  - Access to System Menu
  - Access Learning Management System

- Employee Group Default Behavior Controls
  - Access to System Menu
  - Edit Consent/Privacy Notice
  - Edit Med History Consent
  - Access Learning Management System

- Health Information Management Default Behavior Controls
  - Change Charging Department
  - Edit HIM Diagnosis and Procedure Information
  - Edit and Send Physician Queries
  - Update Problem List
  - Edit Discharge Code

- Edit Medical Record Number
- Edit Service Code
- Edit Subtype
- Edit Patient Type
- Review Medical Necessity
- Edit Consent/Privacy Notice
- Edit Med History Consent
- Edit Exclude from Portal
- Edit Exclude from API
- Edit HIE Shared Data
- Edit Data Sensitivity Level
- Edit Protect Immunization Data
- Access to System Menu
- Link and retitle Information Submissions
- Edit Guarantor Note
- Add New Guarantor Note
- Access Learning Management System

- Laboratory Default Behavior Controls
  - Prompt for Medical Necessity Check
  - Review Medical Necessity
  - Edit Working Diagnosis
  - Ability to edit Receive Information on Hospital Ancillary Orders
  - Collect/Receive Ancillary Orders
  - Edit Consent/Privacy Notice
  - Edit Med History Consent
  - Edit Exclude from Portal
  - Edit Exclude from API
  - Edit HIE Shared Data
  - Edit Data Sensitivity Level
  - Edit Protect Immunization Data
  - Access to System Menu
  - Access Learning Management System

- Licensed Practical Nurse Default Behavior Controls
  - View More Information
  - User is allowed to document
  - User is allowed to complete documents
  - Copy forward documentation
  - Edit Working Diagnosis
  - Administer Medications
  - Be Second Witness
  - Change Diabetic Record
  - Change PCA Protocol
  - Update Problem List
  - Place Telephone Ancillary Orders
  - Place Telephone Medication Orders
  - Place Telephone Nursing Orders
  - Place Protocol Medication Orders
  - Place Protocol Nursing Orders
  - Place Protocol Ancillary Orders
  - Place Verbal Ancillary Orders

- Place Verbal Nursing Orders
- Place Verbal Medication Orders
- Place Written Ancillary Orders
- Place Written Medication Orders
- Place Written Nursing Orders
- Auto-Verify Nursing Orders
- Place Standard Nursing Orders
- Link Orders
- Collect/Receive Ancillary Orders
- Modify Pharmacy Orders
- Access Associated Problem
- Edit Consent/Privacy Notice
- Edit Patient Event Notification Information
- Edit Med History Consent
- Verify Orders
- Edit Exclude from Portal
- Edit Exclude from API
- Edit HIE Shared Data
- Edit Data Sensitivity Level
- Edit Protect Immunization Data
- Create New Visit
- Access to System Menu
- Add/Edit/Remove Allergy
- Copy Forward Notes
- Edit own signed Notes
- Notes CCDA Text Field
- Note Viewing Access
- Note creation access
- Add, Edit, and Remove Surgery
- Template Library Access
- Template Creator Access
- Add and Update Chief Complaint
- Enter Historic/ Resolved Problems
- Access to canned filters
- Phrases Creator Access
- Phrases Library Access
- Phrases Search/Insert Access
- Access Learning Management System
- Submit Prior Authorization
- Add/Edit/Remove Vitals
- Patient Chart - Verify and Unverifiable Actions

- Nursing Staff Default Behavior Controls
  - Create New Visit
  - Admit Patient to Hospital
  - Discharge Patient From Tracking Board
  - User is allowed to document
  - Administer Medications
  - Place Telephone Ancillary Orders
  - Place Telephone Medication Orders
  - Place Telephone Nursing Orders
  - Place Protocol Medication Orders

- Place Protocol Nursing Orders
- Place Protocol Ancillary Orders
- Place Verbal Ancillary Orders
- Place Verbal Nursing Orders
- Place Verbal Medication Orders
- Place Written Ancillary Orders
- Place Written Medication Orders
- Place Written Nursing Orders
- Auto-Verify Nursing Orders
- Place Standard Nursing Orders
- Edit Consent/Privacy Notice
- Edit Patient Event Notification Information
- Edit Med History Consent
- Verify Orders
- Edit Exclude from Portal
- Edit Exclude from API
- Edit HIE Shared Data
- Edit Data Sensitivity Level
- Edit Protect Immunization Data
- Edit ER Log
- Access to System Menu
- Chief Complaint Read Only
- Copy Forward Notes
- Edit own signed Notes
- Notes CCDA Text Field
- Note Viewing Access
- Note creation access
- Problems Read Only
- Surgery Read Only
- Template Library Access
- Template Creator Access
- Phrases Creator Access
- Phrases Library Access
- Phrases Search/Insert Access
- Access Learning Management System
- Submit Prior Authorization
- Add/Edit/Remove Vitals

- Pharmacy Default Behavior Controls
  - Code by Pharmacy
  - Edit Non-HIM Diagnosis and Procedure Information
  - Code by HIM
  - View More Information
  - Edit Working Diagnosis
  - Update Problem List
  - Access Associated Problem
  - Access to System Menu
  - Formulary Matching
  - Remove multiple home medications
  - Place Verbal Medication Orders
  - Place Written Medication Orders
  - Place Protocol Medication Orders

- Enter No Rx Needed Prescriptions Only
- Administer Medications
- Administer Class 3 Thru 5 Substances
- Administer Class 1 Or 2 Substances
- Order Set Setup
- Order List Setup
- Protocol Setup
- Access Learning Management System

- Physician Group Default Behavior Controls
  - Allow Importing Documents
  - Add/Edit Plan of Care
  - View More Information
  - User is allowed to document
  - User is allowed to complete documents
  - Copy forward documentation
  - Save default answers for Clin Doc Documents
  - Sign Documentation
  - Edit Physician Documentation
  - Collect/ Receive Ancillary Orders
  - Modify Pharmacy Orders
  - Access Associated Problem
  - Update Problem List
  - Emergency Access to EPHI
  - Create New Visit
  - Edit Consent/Privacy Notice
  - Edit Patient Event Notification Information
  - Edit Med History Consent
  - Edit Exclude from Portal
  - Edit Exclude from API
  - Edit HIE Shared Data
  - Edit Data Sensitivity Level
  - Create/Reply Secure Messages
  - Access SureScripts History
  - Add Prescribing Physician
  - Approve Prescription Refill Request
  - Discontinue Prescriptions
  - Do Prescription Entry, View, Print
  - Enter No Rx Needed Prescriptions Only
  - Fax Prescriptions
  - Renew Prescriptions
  - Re-print Prescriptions
  - Send Electronic Prescriptions
  - Submit Prior Authorization
  - Select All for Admission destination
  - Select All for Discharge destination
  - Select All for Level of Care destination
  - By-Pass Alternative Med Screen for Formulary Matching
  - Perform Medication Reconciliation to Order Entry
  - Remove multiple home medications
  - Re-Admit
  - Sign Orders

- Order List Setup
- Edit Protect Immunization Data
- Access to System Menu
- Mark other people's signed note erroneous
- Allow no cosignature required option
- Add/Edit/Remove Allergy
- Copy Forward Notes
- Edit other people's draft note
- Edit other people's signed Notes
- Edit own signed Notes
- Notes CCDA Text Field
- Note Viewing Access
- Note creation access
- Add, Edit, and Remove Surgery
- Template Library Access
- Template Creator Access
- Add and Update Chief Complaint
- Access to custom and canned filters
- Add/Edit/Remove Problems
- Phrases Creator Access
- Phrases Library Access
- Phrases Search/Insert Access
- Remember Passphrase
- Access Learning Management System
- Add/Edit/Remove Vitals
- Patient Chart - Verify and Unverifiable Actions

- Radiology Default Behavior Controls
  - Prompt for Medical Necessity Check
  - Review Medical Necessity
  - Edit Working Diagnosis
  - Edit Consent/Privacy Notice
  - Edit Med History Consent
  - Edit Exclude from Portal
  - Edit Exclude from API
  - Edit HIE Shared Data
  - Edit Data Sensitivity Level
  - Edit Protect Immunization Data
  - Access to System Menu
  - Access Learning Management System

- Registered Nurse Default Behavior Controls
  - Add/Edit Plan of Care
  - Create New Visit
  - Admit Patient to Hospital
  - Discharge Patient From Tracking Board
  - View More Information
  - User is allowed to document
  - User is allowed to complete documents
  - Copy forward documentation
  - Edit Working Diagnosis
  - Administer Medications

- Be Second Witness
- Change Diabetic Record
- Change PCA Protocol
- Place Telephone Ancillary Orders
- Place Telephone Medication Orders
- Place Telephone Nursing Orders
- Place Protocol Medication Orders
- Place Protocol Nursing Orders
- Place Protocol Ancillary Orders
- Place Verbal Ancillary Orders
- Place Verbal Nursing Orders
- Place Verbal Medication Orders
- Place Written Ancillary Orders
- Place Written Medication Orders
- Place Written Nursing Orders
- Auto-Verify Nursing Orders
- Place Standard Nursing Orders
- Update Problem List (Problem List), Link Orders
- Collect/Receive Ancillary Orders
- Modify Pharmacy Orders
- Access Associated Problem
- Edit Consent/Privacy Notice
- Edit Patient Event Notification Information
- Edit Med History Consent
- Verify Orders
- Edit Exclude from Portal
- Edit Exclude from API
- Edit HIE Shared Data
- Edit Data Sensitivity Level
- Edit Protect Immunization Data
- Access to System Menu
- Copy Forward Notes
- Edit own signed Notes
- Notes CCDA Text Field
- Note Viewing Access
- Note creation access
- Add, Edit, and Remove Surgery
- Template Library Access
- Template Creator Access
- Add and Update Chief Complaint
- Add/Edit/Remove Allergy
- Enter Historic/Resolved Problems
- Phrases Creator Access
- Phrases Library Access
- Phrases Search/Insert Access
- Re-Admit
- Access to canned filters
- Access Learning Management System
- Submit Prior Authorization
- Add/Edit/Remove Vitals
- Patient Chart - Verify and Unverifiable Actions

- Registration Default Behavior Controls
  - Edit Chief Complaint Fields
  - Edit Consent/Privacy Notice
  - Edit Med History Consent
  - Edit Exclude from Portal
  - Edit Exclude from API
  - Edit HIE Shared Data
  - Edit Data Sensitivity Level (
  - Edit Protect Immunization Data
  - Edit ER Log
  - Update Problem List
  - Edit Guarantor Note
  - Add New Guarantor Note
  - Access Learning Management System

- Rehabilitation Services Default Behavior Controls
  - Prompt for Medical Necessity Check
  - Review Medical Necessity
  - User is allowed to document
  - Edit Working Diagnosis
  - Ability to edit Receive Information on Hospital Ancillary Orders
  - Collect/ Receive Ancillary Orders
  - Access to System Menu
  - Access Learning Management System

- Schedulers Default Behavior Controls
  - Edit Chief Complaint Fields
  - Create/Edit My Schedules
  - Create Appointments
  - Access to System Menu
  - Create/Edit Blocks
  - Create New Visit
  - Access Learning Management System

- System Administrator Default Behavior Controls
  - Allow Importing Documents
  - Add/Edit Plan of Care
  - Create new filters
  - Edit existing filters
  - Modify preferences
  - Modify value of a preference (checked, unchecked)
  - Create New Visit
  - Admit Patient to Hospital
  - Discharge Patient From Tracking Board
  - Edit ER Log
  - Install Updates
  - Send Updates to Test & Train Systems
  - Edit Working Diagnosis (
  - Create And Edit Logins
  - Modify Login And Password Policies
  - Unlock And Reset Passwords

- Create/Edit My Schedules
- Open Charts
- Override Scheduling Blocks
- Order Set Setup
- Order List Setup
- Edit OID Assignment
- Access to System Menu
- SFTP setup
- Send reports using SFTP
- Schedule Reports
- Edit/Cancel Any Scheduled Report
- Copy Forward Notes
- Edit other people's draft note
- Edit other people's signed Notes
- Edit own signed Notes
- Notes CCDA Text Field
- Note Viewing Access
- Note creation access
- Add, Edit, and Remove Surgery
- Template Administrator Access
- Template Library Access
- Template Creator Access
- Access to Notes Admin Tool
- Phrases Administrator Access
- Phrases Creator Access
- Phrases Library Access
- Phrases Search/Insert Access
- Access to custom and canned filters
- Message Configuration

***NOTE**: The Note behavior controls will only become defaults once the Notes application has been activated.*

***NOTE**: The TruBridge Default Behavior Control Rule for each role will be automatically associated with each role. The rule will be associated at the end of the rule list where all rules above will take precedence over it. A deny rule may be created and inserted above the TruBridge default rule if necessary; this will allow flexibility in denying or allowing resources.*

6.5 Data Blocks

This feature is used with the Data Mining application. Please see the Data Mining user guide for more information.

6.6 Screen Defaults

Role Defaults

The following are Screen defaults for each role. No changes may be made to these default settings. If an additional screen needs to be given to a role, a new rule will need to be setup allowing access. If one of the default settings needs to be denied, a new rule will need to be setup denying access. See the Screen 43 section for more information on Screens and instructions on how to add or remove Screens for a specific role.

- Cardiopulmonary Screen Defaults
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Case Management/Social Services Screen Defaults
  - Document Queue View Screen
  - Patient Demographics Panel
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Clinic Staff Screen Defaults
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Employee
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Dietary
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Health Information Management Screen Defaults
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Patient Consent/Privacy Settings
  - Guarantor Note Review
  - Guarantor Note Entry
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Laboratory Screen Defaults
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Licensed Practical Nurse Screen Defaults
  - Document Queue View Screen
  - Patient Demographics Panel
  - Charge Item Lookup
  - Charge Entry
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Nursing Staff Screen Defaults
  - Document Queue View Screen
  - Patient Demographics Panel
  - Charge Item Lookup
  - Charge Entry
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Pharmacy Screen Defaults
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Physician Group Screen Defaults
  - Pharmacies
  - Lookup Caller
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Radiology Screen Defaults
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Registered Nurse Screen Defaults
  - Document Queue View Screen
  - Patient Demographics Panel
  - Charge Item Lookup
  - Charge Entry
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Patient Consent/Privacy Settings
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Rehabilitation Services Screen Defaults
  - Document Queue View Screen
  - Patient Demographics Panel
  - Patient Relationship List
  - Ethnicity Codes List
  - Race Codes List
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- Scheduler
  - Authorization Warning Screen
  - Change Date and Time Screen
  - Login List Screen
  - Lookup Caller Screen

- System Administrator Screen Defaults
  - Document Queue View Screen
  - Patient Demographics Panel

***NOTE**: The TruBridge Default Screen Rule for each role will be automatically associated with each role. The rule will be associated at the end of the rule list where all rules above will take precedence over it. A deny rule may be created and inserted above the TruBridge default rule if necessary; this will allow flexibility in denying or allowing resources.*

6.7 Reports

See the Reports 47 section for more information on report access and instructions on how to add or remove report access for a specific role.

6.8 Custom Reports

This feature is used with the Data Mining application. Please see the Data Mining user guide for more information.

6.9 Filters

The Filters option allows System Administrators to create new filters or edit existing filters and add them to logins or roles. The process for maintaining filters is the same when accessing the Filters option from the Login, Role, or System Administration menu. For more information please see Filters 50.

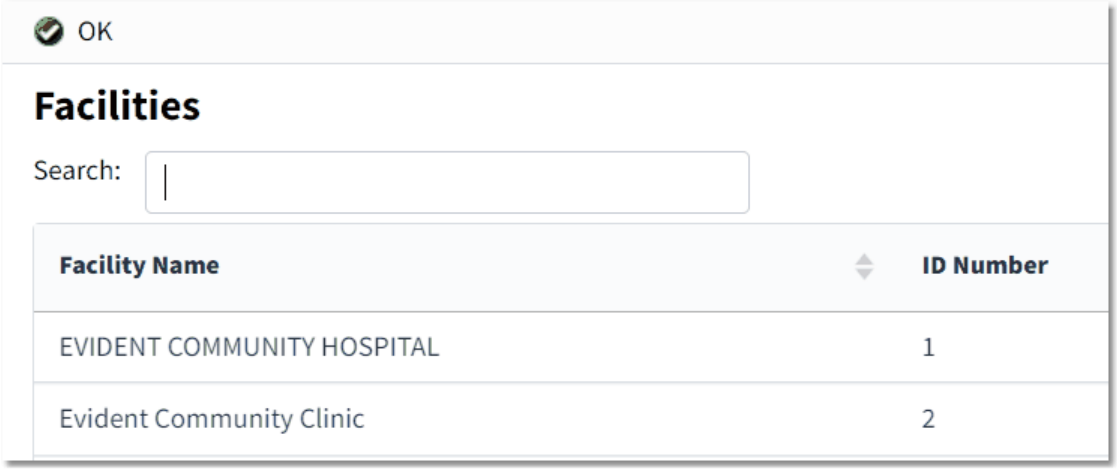
6.10 Events

See the Events 51 section for more information on event set up and instructions on how to add or remove an event for a specific role.

Chapter 7 Facility

Selecting Facility within System Administration will display all active facilities within Thrive.

Select **Web Client** > **System Administration** > **Facility**



System Administration Facility - Application

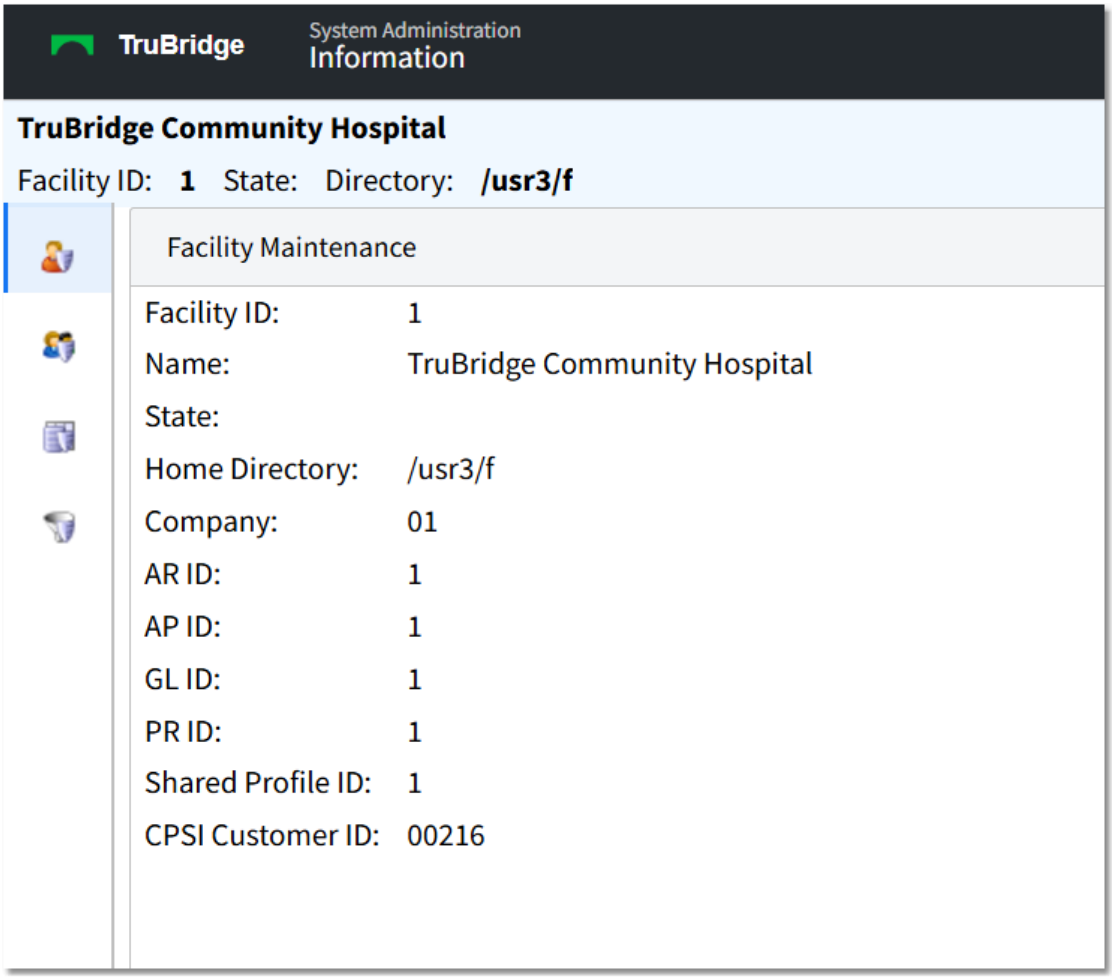
Selecting a facility from the list will allow additional information to display.

NOTE: *Any changes made to the settings will be logged for auditing purposes. This information is stored in the system and may be extracted. Please contact TruBridge support for assistance with this information.*

7.1 Information

Once a facility is selected, the Facility Information screen will display. This is a view only screen displaying the information set up in the facility table.

Select **Web Client** > **System Administration** > **Facility** > **Select Facility** > **Information**



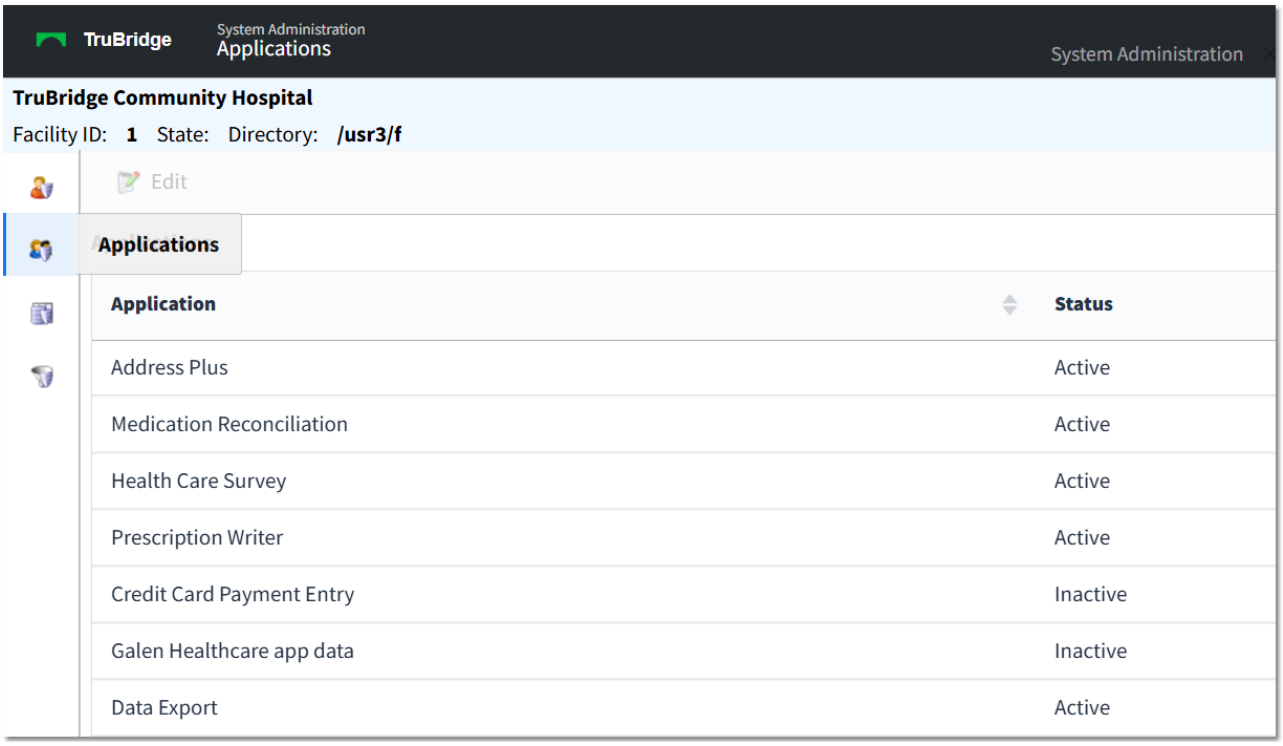
System Administration Facility - Information

7.2 Application

The Application screen will display a listing of Thrive applications. The Status column will display which applications are active or inactive for the selected facility.

NOTE: *Any changes made to the settings will be logged for auditing purposes. This information is stored in the system and may be extracted. Please contact TruBridge support for assistance with this information.*

Select **Web Client** > **System Administration** > **Facility** > **Select Facility** > **Application**



System Administration Facility - Application

7.3 Data Blocks

This feature is used with the Data Mining application. Please see the Data Mining user guide for more information.

7.4 Filters

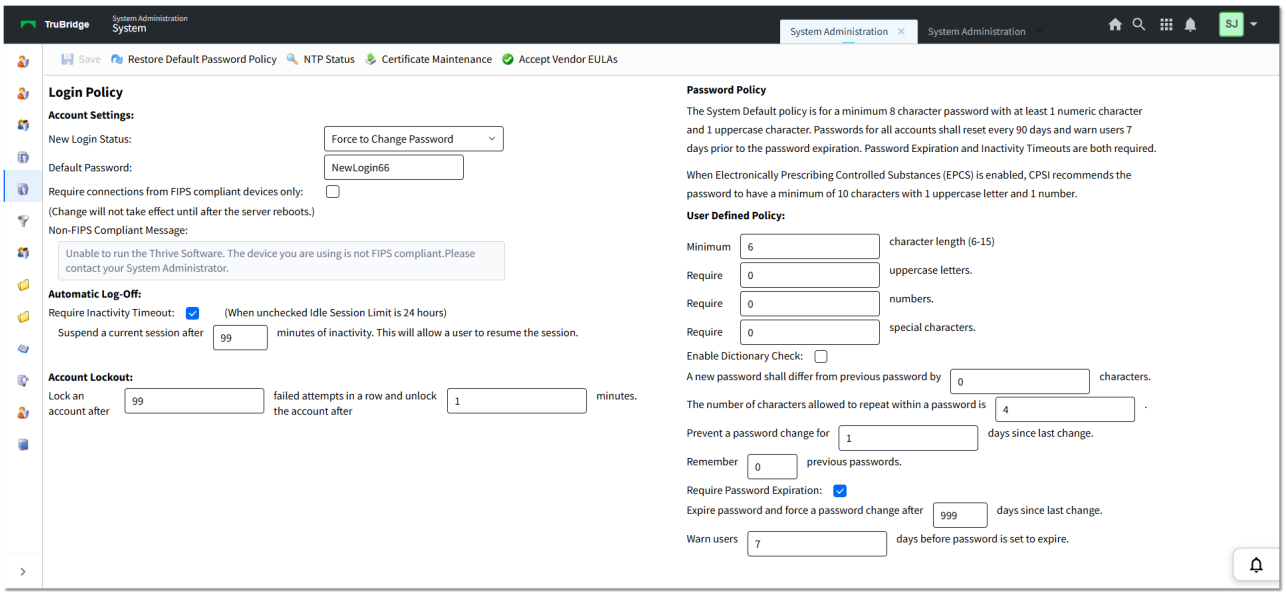
The Filters option allows System Administrators to create new filters or edit existing filters and add them to logins or roles. The process for maintaining filters is the same when accessing the Filters option from the Login, Role, or System Administration menu. For more information please see Filters 50.

Chapter 8 System

The System table is used to set up system-wide login policies based on the preferences of each facility. The facility's System Administrator will maintain this table.

***NOTE**: To make changes to this screen the system administrator's login will need to be in the System Administrator role. By default, the System Administrator role has a behavior control rule allowing it to Create and Edit Logins, Unlock and Reset Passwords and Modify the Login and Password Policies. The behavior control to Modify the Login and Password Policies is what allows this screen to be edited by the System Administrator. If a user's login is not in the System Administrator role, then the login will need to have System Privileges enabled and a behavior control rule allowing them to Modify the Login and Password Policies. The user will also need a screen rule allowing access to the system_edit screen.*

Select **Web Client** > **System Administration** > **System**



System Administration System Security

The following options are available on the action bar.

- **Save:** If any changes are made to any of the fields on the System screen, this option will need to be selected to retain the information. This option will be grayed out until changes have been made on the screen.

- **Restore Default Password Policy:** If selected, all default Thrive Login and Password policies will be restored on the screen. The default policies are set as follows:
  - Login Policy:
    - o New logins forced to change password
    - o Default password will be NewLogin66
    - o Sessions will time out after 10 minutes of inactivity
    - o Accounts will be locked out for 20 minutes after 5 failed attempts to login.

- Password Policy:
  - Minimum of 8 characters
  - At least one numeric character
  - At least one uppercase character
  - Passwords will reset every 90 days
  - Users will be warned 7 days prior to the password expiration

- **NTP Status (Network Time Protocol)**: If selected, the NTP Status screen will display a comparison of the current system time to a trusted time source.

- **Certificate Maintenance**: This option provides a keystore for applications that require a certificate (ex. InterQual).

- **Accept Vendor EULAs**: This option allows End User License Agreements to be viewed and accepted by the System Administrator. For more information, please reach out to a TruBridge technical support representative.

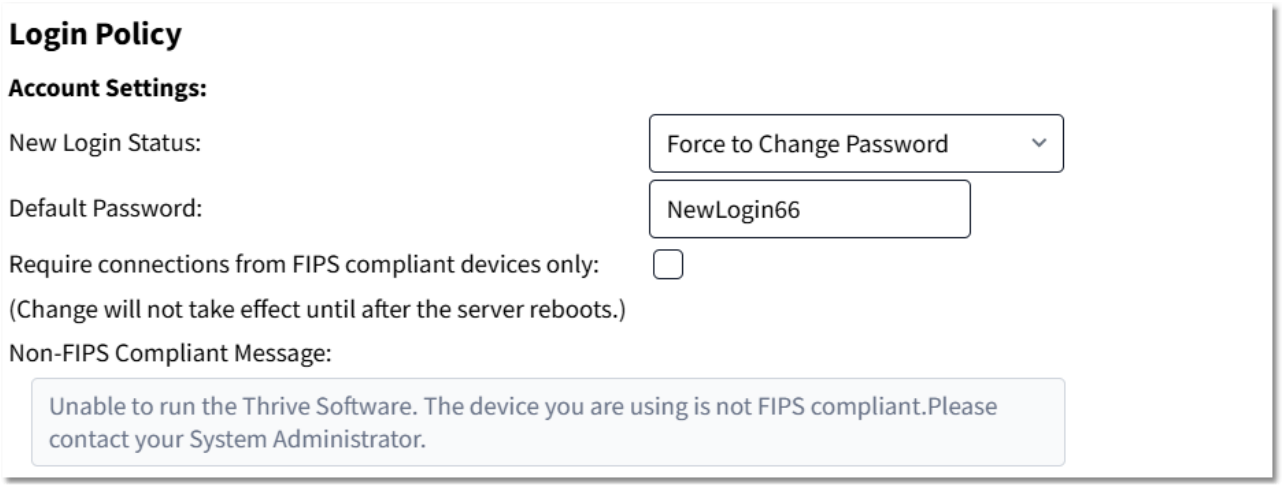
NOTE: *Any changes made to the Login or Password policies will be logged for auditing purposes. This information is stored in the system and can be extracted. Please contact TruBridge support for assistance with this information.*

8.1 Login Policy

The Login Policy allows a facility to define how the user logins may be managed to ensure sensitive information is secure to only allow authorized identities and maintains patient privacy and confidentiality.

Account Settings

Select **Web Client** > **System Administration** > **System**



Login Policy - Account Settings

- **New Login Status:** This option will define what the default status will be for newly created logins.
  - Force to Change Password: When a login is created, the user must enter the default password and will then be prompted to create a new one.
  - Disabled: When a login is created, the status will default to disabled. The IT administrator will need to enable the login before it may be used. Once the login has been enabled, the user must enter the default password and will then be prompted to create a new one.

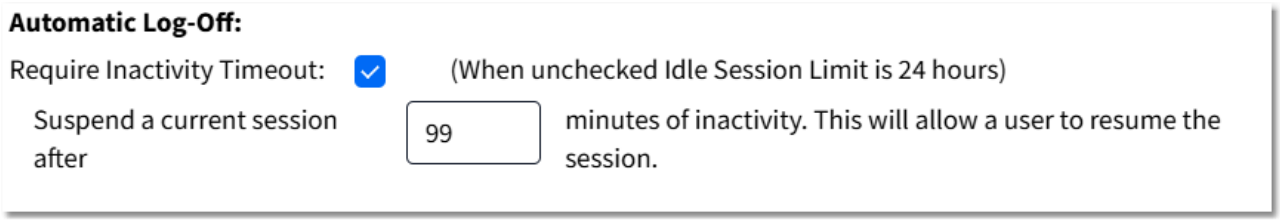
- **Default Password:** The password entered in this field will be used for logging into the system for the first time to create a password. It will also be used when a login has been reset.

- **Require connections from FIPS compliant devices only:** When this field is checked, the system looks at the PC's Security Policies to determine if the PC is FIPS Compliant. If the PC is compliant, the user will be able to log into Thrive as normal. If the PC is not FIPS Compliant, the user will receive the message listed in the subsequent field for Non-FIPS compliant devices.

- **Non-FIPS Compliant Message:** When **Require connections from FIPS compliant devices only** is enabled, the system will automatically populate this field with the default message, "Unable to run the Thrive Software. The device you are using is not FIPS compliant. Please contact your System Administrator." This field is a free-text field and may be edited with any message so desired up to 125 characters. Only a user that is in the System Administration group may save changes to these fields.

Automatic Log-Off

Select **Web Client** > **System Administration** > **System**



Login Policy - Automatic Log-Off

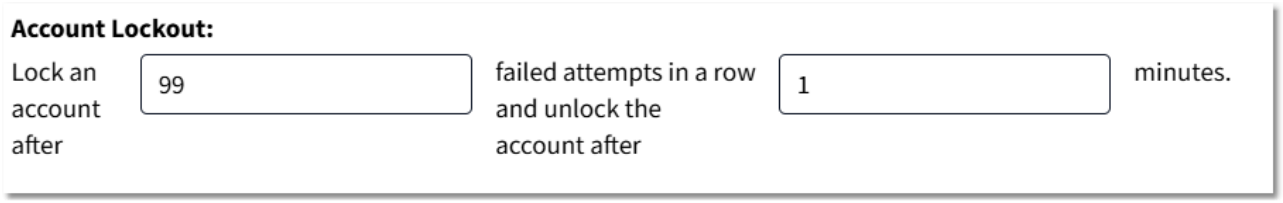
- **Require Inactivity Timeout**: This security setting will be enabled by default. If this option is disabled (unchecked), an attestation disclaimer will display. The message will display, "This control is enabled by default for the Thrive EHR. By disabling the Security Control, the user is attesting that another technical control adequately addresses or exceeds in addressing threat/vulnerabilities related to password authentication and user identification. Are you sure you want to continue?" If **No** is selected, the setting will remain enabled. If **Yes** is selected, the setting will be disabled; the 'Suspend a current session after X minutes of inactivity' will be set to -1 indicating that there is no system level inactivity timeout currently set. Role and user level inactivity timeouts may still be enforced even when the system level timeout is disabled via this option. If disabled, the user's sessions will lock when idle for up to 24 hours, provided no role or user level inactivity timeout is defined.

- **Suspend a current session after ___ minutes of inactivity. This will allow a user to resume the session:** The number of minutes of inactivity that must be met before a user is logged off the system. Once logged off, the user will be able to enter the password for that login to resume the session. The Auto Sign-off field in Department Security will override this setting.

- **End a current session after ___ minutes of inactivity. This will completely disconnect the session:** Programmed for future release.

Account Lockout

Select **Web Client** > **System Administration** > **System**



Login Policy - Account Lockout

- **Lock an account after ___ failed attempts in a row and unlock the account after ___ minutes:** The number of tries a user may enter an incorrect password before being locked out. If the user has met the number of failed attempts, the account may be locked out of the system for a certain number of minutes. Once those minutes have been met, users may try and enter in the password again.

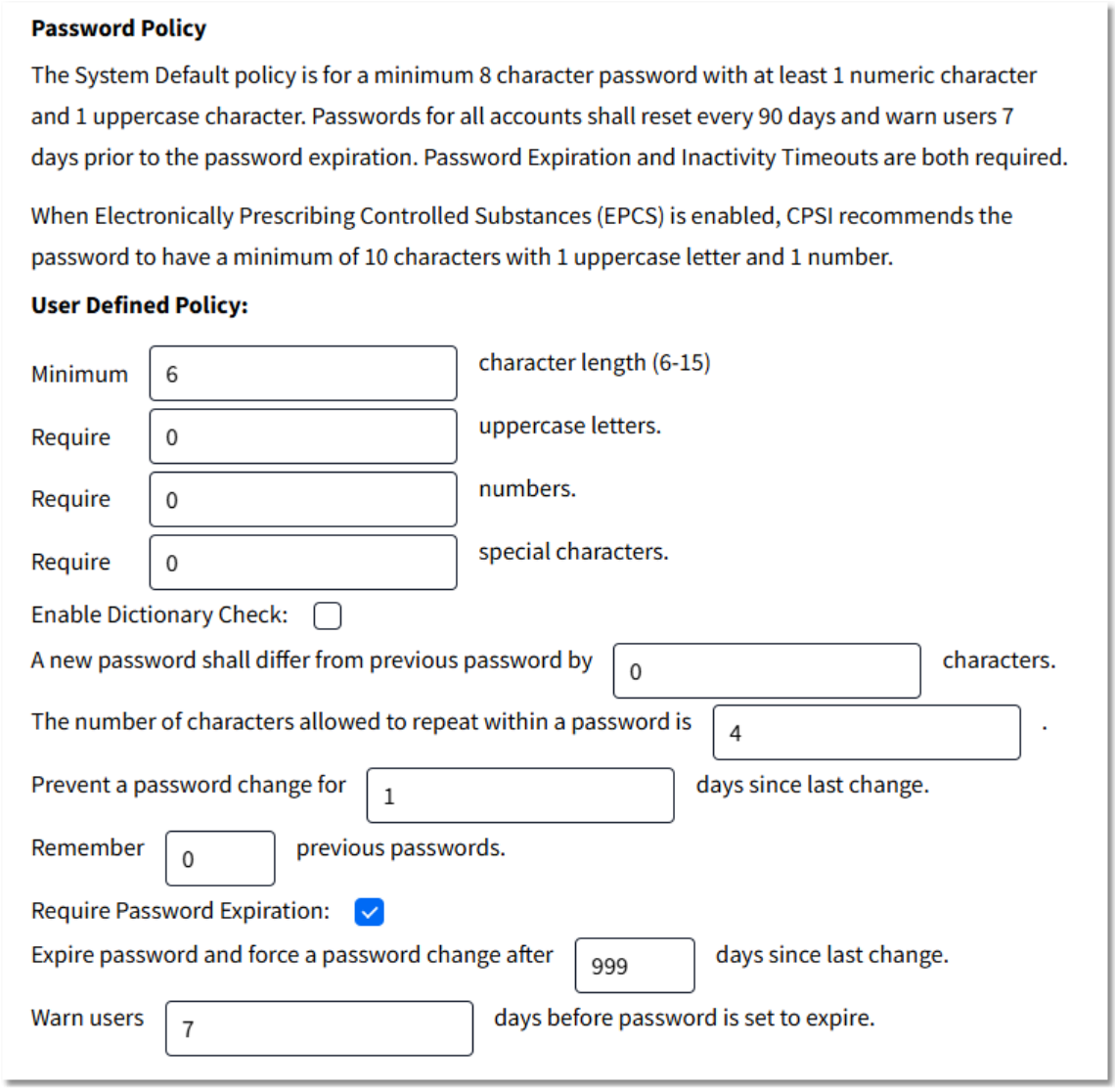
NOTE: *If 00 minutes is loaded for the lockout minutes, the System Administrator will need to manually unlock the user.*

8.2 Password Policy

The Password Policy section allows facilities a means to employ technical security standards that prevent unauthorized access to the system and assist to mitigate common security problems to sensitive information.

User Defined Policy

Select **Web Client** > **System Administration** > **System**



User Defined Policy

- **Minimum Character Length (6-15):** The minimum amount of characters for a password. This number will need to be a minimum of 6 and a maximum of 15.

- **Require Uppercase Letters:** The required number of uppercase letters in the password. This number may be 0-9.

- **Require Numbers:** The required number of numbers in the password. This number may be 0-9.

- **Require Special Characters:** The required number of special characters in the password. This number may be 0-9.

- **Enable Dictionary Check:** Select this option to check the user's password against any possible words that may be found in a dictionary. If this option is not selected, the user may set up a password based on a dictionary word as long as it meets the other password requirements.

NOTE: *When Enable Dictionary Check is selected, passwords are checked for complexity against a dictionary of known easily guessable passwords and not a language dictionary. What may not be a word to humans may actually be an easily guessable password based upon common intrusion techniques and known security issues.*

- **A new password shall differ from previous password by ___ characters:** The required number of characters that need to differ between a user's new password and previous password. For example, if the characters need to differ by two characters, and the old password was Thrive1234, a new password of Thrive1235 would not be accepted, but a new password of Thrive1255 would be accepted. This number may be 0-4.

- **The number of characters allowed to repeat within a password is ___:** The required number of times a character is allowed to be repeated in a password. For example, if only two characters are allowed to be repeated, Banana would not be accepted because the "a" is used more than twice.

- **Prevent a password change for ___ days since last change:** The required number of days that have to be met before a user can change their password. This number may be 1-30.

- **Remember ___ previous passwords:** The required number of previous passwords that cannot be used when creating a new password.

- **Require Password Expiration**: This security setting will be enabled by default. If this option is disabled (unchecked), the following attestation disclaimer will display: "This control is enabled by default for the Thrive EHR. By disabling the Security Control, the user is attesting that another technical control adequately addresses or exceeds in addressing threat / vulnerabilities related to password authentication and user identification. Are you sure you want to continue?" If **No** is selected, the setting will remain enabled. If **Yes** is selected, the setting will be disabled; the 'Expire password and force a password change after X days since last change' and 'Warn users X days before password is set to expire' fields will be set to -1 indicating that there is no password expiration currently set. When disabled, user accounts will not have their passwords expire. This is only appropriate in a single sign-on environment where device level access controls are in place.

- **Expire password and force a password change after ___ days since last change:** The number of days a password will expire from when it was last changed. When the password expires, the user will be forced to then set up a new password that meets the password requirements. This number may be 1-999.

- **Warn users ___ days before password is set to expire:** The number of days a warning message will start to appear for a user. The warning will inform the user of how many days until the password expires.

***NOTE**: All login credentials created by end users in Thrive that follow the password properties described above, are hashed using an SHA512 algorithm. Once hashed, the original keyed in password is discarded and not stored in any form, text or otherwise. Instead, the resulting hash is safely stored by Thrive EHR Server OS. When a user signs on and keys in their secret knowledge factor, or password, it is immediately hashed and compared to the hash created when the password was originally set.*

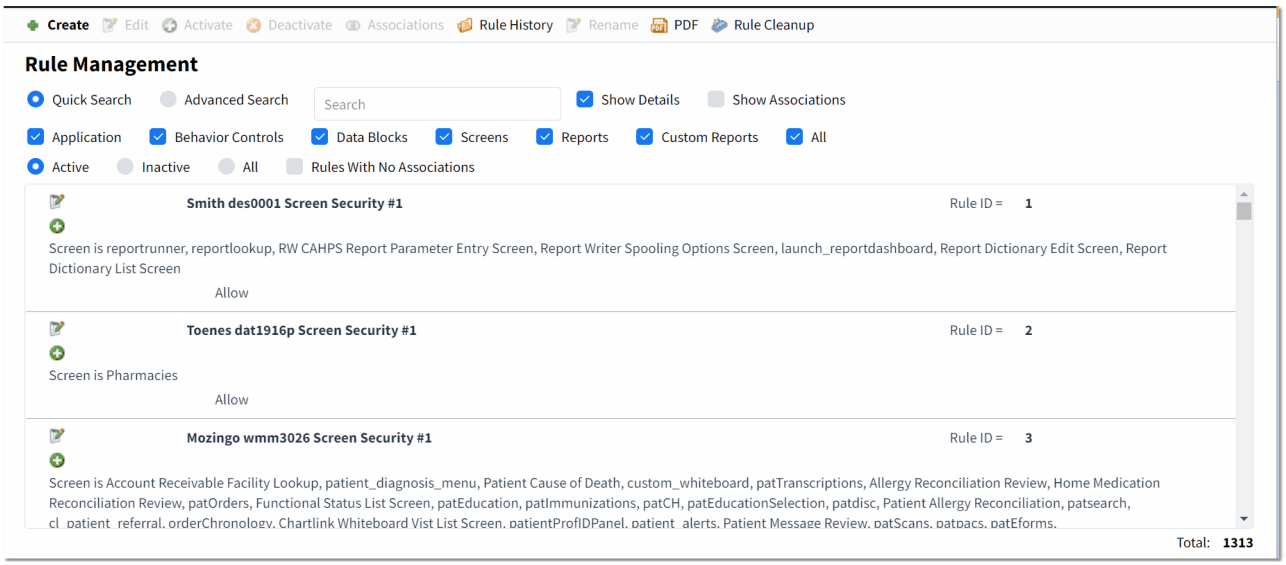
Chapter 9 Filter

The Filters option allows System Administrators to create new filters or edit existing filters and add them to a login or role. The process for maintaining filters is the same when accessing the Filters option from the Login, Role, or System Administration menu. For more information please see the Filters 50 section of this documentation.

Chapter 10 Rule Management

The Rule Management option offers a universal rule listing that includes all Application, Behavior Controls, Data Blocks, Screens, Reports, and Custom Report rules. From here, new rules may be created and existing rules may be associated with multiple entities (logins and roles).

Select **Web Client** > **System Administration** > **Rule Management**



Rule Management

Search Options

Advanced search options are available on the rule listing making it easier to find and manage rules. The following options are available:

- **Quick Search**: Allows rules to be searched by Rule Title and Rule ID. This search feature will NOT search the Rule Details.
- **Advanced Search**: Allows rules to be searched by Rule Title, Rule ID, and Rule Details. When using this option, a **Search** optuon will appear on the action bar. This must be selected before search results will display. When combined with the Show Associations option, a login may be entered in the search field to search for rules associated with a specific user.
- **Show Details**: When selected, the Rule Details will display. When not selected, only the Rule Title will display.
- **Show Associations**: When selected, the entities associated with the rule will display. When combined with the Advanced Search option, a login may be entered in the search field to search for rules associated with a specific user.

- **Rule Type Filters**: Select the types of rules that should display in the search results. Options are: Application, Behavior Controls, Data Blocks, Screens, Reports, and Custom Report rules.
- **Active/Inactive/All Filters**: Select **Active** to display only active rules. Select **Inactive** to display rules that have been deactivated. Select **All** to display both active and inactive rules.
- **Rules with No Associations**: Select this option to only display rules that have no logins or roles associated to them.

Rule Management Tools

The following tools are available to assist with Rule Management.

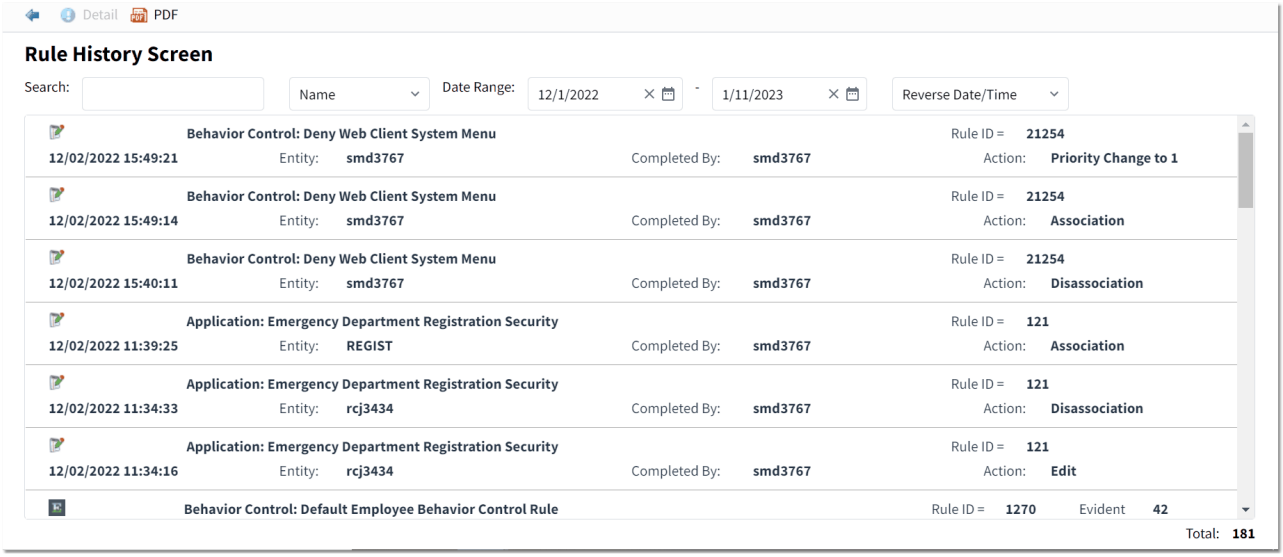
- **Create**: Allows new rules to be created and added to the rule listing. When selected, the system will prompt for the type of rule to be created (ex. Application, Behavior Control, etc.). Once a rule is created, it may be added to an entity using the Associations option on the Rule Management screen.
- **Edit**: Allows the details of the selected rule to be edited.
- **Activate**: Allows inactive rules to be reactivated. Keep in mind that reactivating a rule will not re-associate it with the entities it was previously associated with.
- **Deactivate**: Allows active rules to be deactivated. Deactivating a rule will disassociate the rule from all entities currently tied to it. Deactivated rules will display in the Inactive list.
- **Associations**: Displays the users or roles currently associated with the rule. From here, an **Add Association** option is available that will allow additional users or roles to be added to the rule. Once selected, double-click the user(s) or role(s) that should be associated with the rule. This will add them to the Pending column. Select **Update Pending** to associate the entities to the rule.
- **Rule History**: Displays a list of changes made to any rule in System Administration. Changes recorded in Rule History are the association or disassociation of users or roles to a rule, the addition of or removal of a resource to a rule, and the activation or inactivation of a rule. For more information, please see the Rule History 104 section.
- **Rename**: Allows the title of the selected rule to be edited.
- **PDF**: Creates a PDF document of the displayed search results.
- **Rule Cleanup**: Provides a way to identify duplicate rules and consolidate them into one rule. See the Rule Cleanup 106 section for more information.

10.1 Rule History

Rule History will display a list of changes made to any rule in System Administration. Changes recorded in Rule History are the association or disassociation of users or roles to a rule, the addition of or removal of a resource to a rule, and the activation or inactivation of a rule. The following will be displayed along with each change: the date/time the change was made, the login or role that the change was made to, and the login that completed the changes.

A search feature is available that allows Rule History to be searched by the login that made the change, the Entity (login/role) that was changed, the Rule ID, or the Action that was taken. A date range may be entered to search for a specific time frame. The Sort By option allows the information on the screen to be sorted by: Action, the login that made the change, the date/time the change was made (Newest to Oldest changes), the Entity that was changed, the Name of the rule, the reverse date/time (Oldest to Newest changes), or the Type of Rule (Application, Screen, Report, Behavior Control, Events, Data Blocks, Components, Custom Reports).

Select **Web Client** > **System Administration** > **Rule Management** > **Rule History**



Rule History Screen

The following information is displayed on the screen.

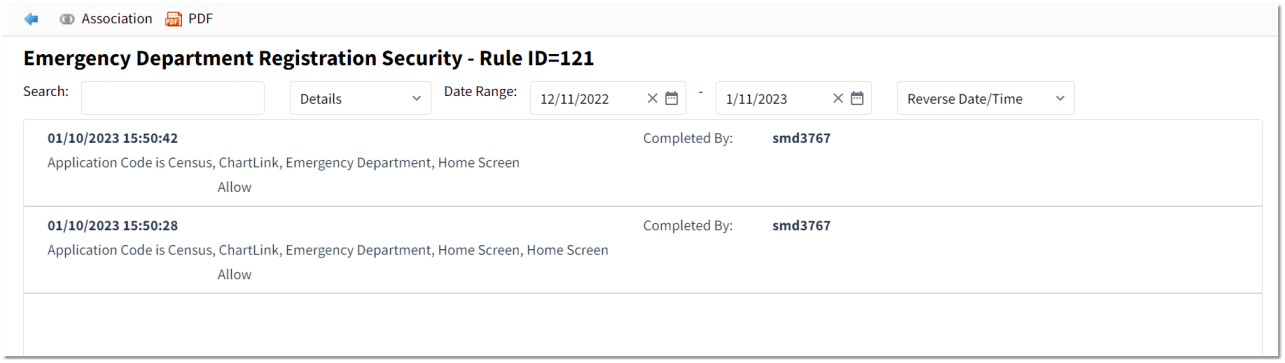
- **Rule Type/Title**: Displays the type of rule (Application, Screen, Report, Behavior Control, Events, Data Blocks, Components, Custom Reports) followed by the rule title.
- **Rule ID =** : This is a unique identification number that is assigned to the rule when it is created.
- **Date/Time**: The date/time that the change was made to the rule.
- **Entity**: The login or role where the rule was changed.
- **Completed By**: The login that made the change to the rule.

- **Action**: Defines how the rule was changed. The following actions will display.
  - **Edit**: Displays when a new rule is created or when an existing rule has the title or details changed, it will also display when a rule is activated or deactivated.
  - **Association**: Displays when the rule is associated with a new entity.
  - **Disassociation**: Displays when the rule is disassociated with an entity.
  - **Priority Change to X**: Displays when the Change Order option is used to edit the priority of the rule for the entity. This action will display as Priority Change to X, where X is the new Priority of the rule.

Details

The Details option may be used to see a list of changes made to the rule. When a change is made to a rule, the updated version of the rule will be displayed at the top of the rule history list. Thrive will continue to track any additional changes made to the rule, the list will display the newest version of the rule a the top of the screen and the oldest version at the bottom of the screen. Search tools are available to help identify specific changes.

Select **Web Client** > **System Administration** > **Rule Management** > **Rule History** > **Select Entry** > **Details**



Rule History - Details

The following information displays on the screen:

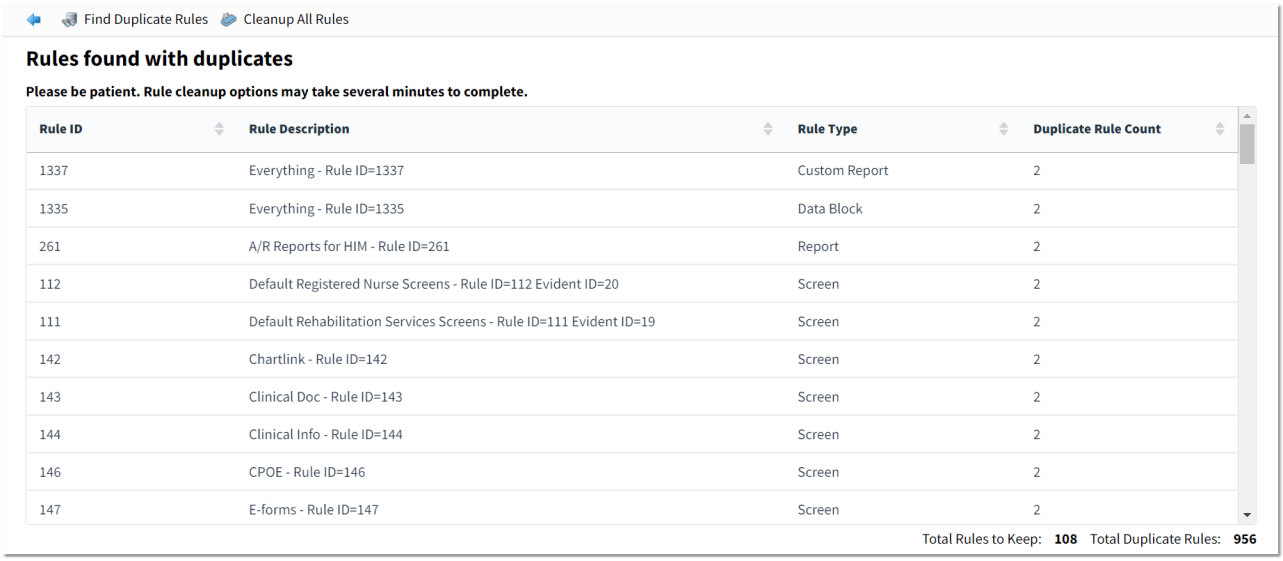
- **Date/Time**: The date/time that the change was made to the rule.
- **Rule Details**: Shows the application, screen, report, or behavior controls that are either allowed or denied by the rule.
- **Completed By**: The login that made the change to the rule.

10.2 Rule Cleanup

The rule cleanup option may be used to identify duplicate rules and consolidate them into one rule. From System Administration, select **Rule Management**, **Rule Cleanup**, then select **Find Duplicate Rules**.

A list of rules will display. These are the rules that will be kept if the Cleanup All Rules option is selected. When evaluating duplicate rules, the system will use the rule with the most associations as the Rule to Keep. Selecting **Cleanup All Rules** will deactivate all duplicate rules and the entities assigned to the duplicate rules will be associated with the Rule to Keep.

Select **Web Client** > **System Administration** > **Rule Management** > **Rule Cleanup** > **Find Duplicate Rules**



Find Duplicate Rules

Double-clicking a single rule from the list will display the details for the Rule to Keep. From here, the rule Description (Title) may be updated, and the details of the rule will display along with the Matching Rules (Duplicate Rules). Selecting **Cleanup** will deactivate the Matching Rule(s) and the entities assigned to the Matching Rule(s) will be associated with the Rule to Keep.

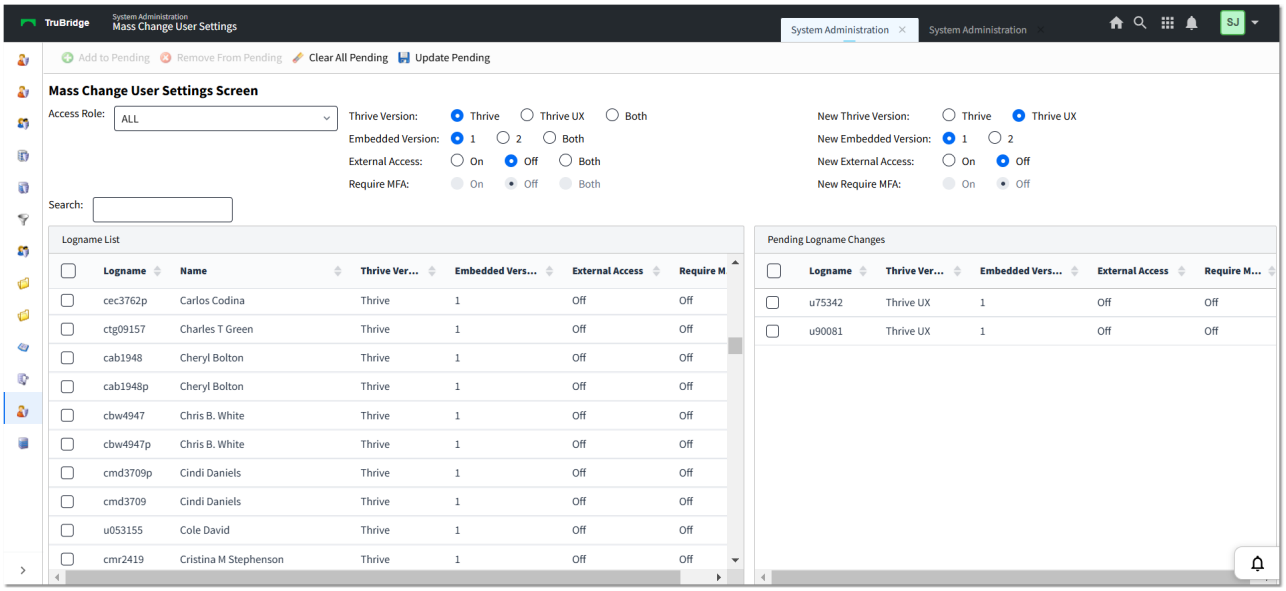
Select **Web Client > System Administration > Rule Management > Rule Cleanup > Find Duplicate Rules > Select Rule**

Rule to Keep

Chapter 11 Mass Change User Settings

The Mass Change User Settings Screen allows the Thrive Version, Embedded Version, External Access and Require MFA options to be assigned to multiple logins at one time. To make changes using this table, the login must have the behavior control, Create and Edit Logins set to Allow.

Select **Web Client** > **System Administration** > **Mass Change User Settings**



Mass Change User Settings Screen

To begin, use the filter features to display a list of logins in Logname List. The following filter options are available:

- **Access Role**: Select a role from the drop-down menu to view logins associated with a specific role.
- **Thrive Version**: Select a Thrive Version to only view logins with the selected Thrive Version.
- **Embedded Version**: Select an Embedded Version to only view logins with selected Embedded Version.
- **Search**: Use this option to search for a specific login by Logname or Name.

Double-click the logins from the Logname List to add them to the Pending Logname Changes list.

Then select the **New Thrive Version**, **New Embedded Version**, **New External Access**, and/or **New Required MFA.**

- **New Thrive Version:** If Thrive UX is selected, the login will only be able to login using Thrive UX. If Thrive is selected, the user will have the option of choosing Thrive or Thrive UX.

- **New Embedded Version**: The embedded version will determine how users will view embedded screens within Thrive UX.

- **New External Access**: If **On** is selected, the user may access the EHR via the Web Client when connecting both in and out of the facility's network. Once selected, the 'New Require MFA' option will become available to set for users. When **Off** is selected, the user may only access the EHR via the Web Client when in the facility's network; the user will be denied access when out of network. Refer to the Multi-Factor Authentication 135 section for more information.

- **New Require MFA**: If **On** is selected, a One-Time Password (OTP) is required when accessing the EHR via the Web Client when connecting out of network. This option is only available when external access to the Web Client is allowed (see previous field). When this option is not selected, a OTP is not required when accessing the EHR via the Web Client. Refer to the Multi-Factor Authentication 135 section for more information.

Next, choose **Update Pending** to assign the New Version(s) to the logins.

Additional options are available on the action bar, below is an explanation of each.

- **Add to Pending**: Select a login from the Logname List then select Add to Pending to move the login to the Peding Logname Changes list.

- **Remove from Pending**: Select a login from the Pending Logname Changes list, then select Remove from Pending to delete a login from the Pending Logname Changes list.

- **Clear All Pending**: Select this option to remove all logins from the Pending Logname Changes list.

- **Update Pending**: Select this option to update all logins in the Pending Logname Changes list to the New Thrive Version and New Embedded Version.

Chapter 12 Behavior Control Definitions

This section defines what each Behavior Control in System Administration does throughout Thrive.

12.1 3R Management Suite

- **Upload 3R Management Suite Entries:** When set to allow, this will allow the 3R Management Suite option to display in the Patient Charging and General Ledger Review/Correct screens.

12.2 Appointment Reminders/Confirmations

- **Message Configuration:** When set to allow, users will have access to the Messages option within the General Controls table. This will allow messages sent via the Patient Connect application to be customized. When set to deny, users will not have access the Messages option.

12.3 Auditing

- **Audit access for Accounting Role**: When set to Allow, access will be given to Change Log information for the tables assigned to the Accounting database access role.
- **Audit access for Accounts Receivable Role**: When set to Allow, access will be given to Change Log information for the tables assigned to the Accounts Receivable database access role.
- **Audit access for Payroll Role**: When set to Allow, access will be given to Change Log information for the tables assigned to the Payroll database access role.
- **Audit access for Time and Attendance Role**: When set to Allow, access will be given to Change Log information for the tables assigned to the Time and Attendance database access role.
- **Audit access for Patient Clinical Information Role**: When set to Allow, access will be given to Change Log information for the tables assigned to the Patient Clinical Information database access role.
- **Audit access for Table Maintenance Role**: When set to Allow, access will be given to Change Log information for the tables assigned to the Table Maintenance database access role.
- **Audit access for Unassigned DB Role**: When set to Allow, access will be given to Change Log information for the tables that have not been assigned to a database access role.

12.4 Big Brother

- **BB Third Party Vendor Allow Functionality**: TruBridge Use Only.
- **Edit Client Access for Division**: TruBridge Use Only.

12.5 Census

- **Add New Guarantor Note:** When set to Allow, Guarantor Notes may be added to a patient's account.
- **Admit Patient to Hospital:** When set to Allow, access will be given to allow patients to be admitted from the Patient Location Maintenance screen in the Tracking Board.
- **Create additional races and ethnicities during registration:** When set to Allow, access will be given to create and add new races and/or ethnicities from the profile or visit.
- **Create New Visit:** When set to Allow, access will be given to allow patient registration to be handled from the Tracking Board.
- **Discharge Patient From Tracking Board:** When set to Allow, access will be given to allow patient to be discharged from the Patient Location Maintenance screen in the Tracking Board.
- **Edit Chief Complaint Fields:** When set to Allow, access will be given to all the fields on the chief complaint screen. If access has not been given, or it has been denied, the fields on the screen will be grayed out.
- **Edit Consent/Privacy Notice:** When set to Allow, access will be given to the "Consent/Privacy Notice" field in the Consent/Privacy Settings screen. This field will determine if the Consent/Privacy form was signed by the patient.
- **Edit Data Sensitivity Level:** When set to Allow, access will be given to the "Data Sensitivity Level" field in the Consent/Privacy Settings screen. This field will determine the sensitivity level of the patient's data. If access has not been given, or it has been denied, this field will be grayed out.
- **Edit Discharge Code:** When set to Allow, access will be given to the Discharge Code field on the Demographics - Encounter screen and will allow the Discharge Code to be changed if necessary. When set to Deny, the Discharge Code field will be inaccessible.
- **Edit ER Log:** When set to Allow, access will be given to the "Update" option in the ER Log to save new information on the screen. If access is not given, the "Update" option will be greyed out.
- **Edit Exclude from API:** When set to Allow, access will be given to the "Exclude from API" field in the Consent/Privacy Settings screen. This field is for future use. If access has not been given, or it has been denied, this field will be grayed out.

- **Edit Exclude from Portal:** When set to Allow, access will be given to the "Exclude from Portal" field in the Consent/Privacy Settings screen. This will prevent the patient's visit information from displaying in the Patient Portal. If access has not been given, or it has been denied, this field will be grayed out.

- **Edit HIE Shared Data:** When set to Allow, access will be given to the "HIE Shared Data" field in the Consent/Privacy Settings screen. This field will determine if the patient's visit information may be shareable with an RHIO. If access has not been given, or it has been denied, this field will be grayed out.

- **Edit Guarantor Note:** When set to Allow, Guarantor Notes may be edited on a patient's account.

- **Edit Medical Record Number:** When set to Allow, access will be given to the Medical Record number field on the Demographics - Personal screen and will allow the Medical Record number to be changed if necessary. When set to Deny, the Medical Record number field will be inaccessible.

- **Edit Med History Consent:** When set to Allow, access will be given to the "Med History Consent" field in the Consent/Privacy Settings screen. This field represents the consent level to be utilized when retrieving medication history.

- **Edit Patient Event Notification Information:** When set to Allow, access will be given to add, edit or delete physicians from the Care Team Event Notification screen. When set to Deny, users will have view only access to the Care Team Event Notification screen.

- **Edit Patient Type:** When set to Allow, access will be given to the Patient Type field on the Demographics - Encounter screen and will allow the Patient Type to be changed if necessary. When set to Deny, the Patient Type field will be inaccessible.

- **Edit Protect Immunization Data:** When set to Allow, access will be given to the "Protect Immunization Data" field in the Consent/Privacy Settings screen. This field will determine if a patient's immunization data may be shared. If access has not been given, or it has been denied, this field will be grayed out.

- **Edit Service Code:** When set to Allow, access will be given to the Service Code field on the Demographics - Encounter screen and will allow the Service Code to be changed if necessary. When set to Deny, the Service Code field will be inaccessible.

- **Edit Subtype:** When set to Allow, access will be given to the Subtype field on the Demographics - Encounter screen and will allow the Subtype to be changed if necessary. When set to Deny, the Subtype field will be inaccessible.

12.6 Change Management

- **Install Updates**: When set to Allow, the **Install** option is available and allows the user to install updates. When set to Deny, the **Install** option will not be available to the user.
- **Send Updates to Test & Train Systems**: When set to Allow, the **Send Updates** option is available for the user to send updates to the site's training server. When set to Deny, the **Send Updates** option is unavailable to the user.

12.7 Charge Entry

- **Delete Anesthesia Times and Basic Values:** When set to Allow, the user has the ability to delete anesthesia times and basic values from the Anesthesia screen.
- **Delete Drug Waste**: When set to Allow, the user has ability to delete a medication waste entry on the Medication Waste screen from Charge Entry.
- **Edit Anesthesia Times and Basic Values:** When set to Allow, the user has the ability to make changes to the anesthesia times and basic values on the Anesthesia Edit screen.
- **Edit Drug Waste**: When set to Allow, the user has ability to edit the amount of medication waste on the Medication Waste screen from Charge Entry.
- **Change Charging Department**: When set to Allow, the user has ability to change the charging department in the charge edit screen within the Charge Entry application.
- **Change Charge Entry Department**: When set to Allow, the user has ability to change the department on the charge entry screen regardless if the patient is in a room or not.

12.8 ChartLink

- **Emergency Access to EPHI:** When set to Allow, users may access patient medical information in the event of an emergency. The users will receive the Emergency Access Unauthorized Screen, this screen displays an unauthorization statement including an acceptance disclaimer regarding emergency access and the responsibility for their actions.
- **Show Sub Accounts**: When set to Allow, allows Critical Access Hospital sub accounts to display for the user. When set to Deny, access to Critical Access Hospital sub accounts do not display for the user. The default for this rule is set to Deny.

12.9 Clinical Information

- **Edit Working Diagnosis**: When set to Allow, this allows users to access the Working Diagnosis fields on the Patient Diagnosis Screen via the Admitting Diagnosis option found on the Diagnosis/Physicians tab in a patient's Clinical Information page.

12.10 Coding

- **Code by HIM:** When set to allow, access will be given to the Diagnosis, Admitting Diagnosis, Reason for Visit and Procedures screens in the Grouper. This will only allow these screens to be viewed, additional behavior controls are required to edit the information on these screens. When set to deny, the Grouper will be inaccessible, and coding will be done in the DRG Grouper and Maintenance screen.

- **Code by Insurance:** When set to allow, access will be given to the Insurance Diagnosis, Insurance Admitting, and Insurance Procedures screens in the Grouper. This control will only allow these screens to be viewed, additional behavior controls are required to edit the information on these screens.

- **Code by Pharmacy:** When set to Allow, the user has the ability to access the RX Diagnoses screen and the Pharmacy drop-down menu option. Access will also be given to add and edit diagnoses on the Pharmacy screen for the purpose of Disease-Interaction Checking. Neither the Grouper nor the Problem List are updated with these diagnoses.

- **Coding by Lab:** When set to Allow, view only access will be given to the Diagnosis Maintenance screen in the Pathology/Cytology Application. The Edit Non-HIM Diagnosis and Procedure Information behavior control is required to add new diagnoses or delete current diagnoses on this screen.

- **Coding by TruBridge - CPSI USE ONLY:** TruBridge use only

- **Edit and Send Physician Queries**: When set to allow, the user has the ability to edit and send Physician Queries. The user will also have the ability to delete a query they created that is at a status of "Awaiting Physician".

- **Edit HIM Diagnosis and Procedure Information:** When set to allow, access will be give to all action buttons available on the Diagnosis, Admitting Diagnosis, Reason for Visit and Procedures screens in the Grouper.

- **Edit Non-HIM Diagnosis and Procedure Information:** When set to Allow, access will be given to all action buttons available on the Insurance Diagnosis, Insurance Admitting, and Insurance Procedures screens in the Grouper.

12.11 Data Analytics

- **Create/Edit Personal Configuration**: When set to Allow, the user or role may edit any existing component, even if the component was created by another user. When set to Deny, the user or role may not edit any existing components.

- **Edit Any Existing Configuration**: When set to Allow, the user or role may create a new component and add it to his or her dashboard. When set to Deny, the user or role is not able to create a new component.

12.12 Data Dictionary

- **Perform Shared Table Maintenance**: When set to Allow, this will allow users to add or remove tables within the Copy and Share screens in the Data Dictionary. It will also allow users to Share or Unshare, or Add or Remove Exceptions on the Sharing screen.

- **Toggle Auditing**: When set to Allow, this will allow users to check or uncheck the Audit field in the Data Dictionary. The Audit fields will only be able to be accessed if the TruBridge Required field is not checked.

12.13 Diagnostic Imaging AUC Consultation

- **Prompt for Imaging Consultation**: When set to Allow, users will be prompted for the CDSM (AUC) during the Order Entry process when the appropriate diagnostic imaging test is selected.

- **Require AUC Imaging Consultation**: When set to Allow, users will be required to enter the AUC Consultation information during the Order Entry process before saving the order.

12.14 Documentation

- **Amend Clinical Documentation For Any Login:** When set to Allow, the user has the ability to amend flow chart or documentation data entered via another user. The default is deny. Options include Change date and time for all entries in current section or entire document, Amend all entries for this document, and Remove all entries for this section or document.

NOTE: *Currently the Super Amend Functionality does not allow amending Vital Sign documentation by another user.*

- **Copy Forward Documentation:** When set to Allow, the user has the ability to copy forward questions that are flagged in setup to copy forward documentation from visit to visit.

- **Edit Instructions:** When set to Allow, the user has the ability to Create New Instructions, Edit Instructions and Delete Instructions from the Instruction table.

- **Save Default Answers for Clin Doc Documents:** When set to Allow, the user has the ability to save and apply default answers.

- **Sign Documentation:** When set to Allow, the user has the ability to sign documentation and reports and allows access to Key Maintenance to create or change the user's passphrase.

- **Skip required questions in documentation**: When set to Allow, the user has the ability to skip questions in documentation which are set up as required or warning in order to continue documenting in additional sections. The user, however, is prompted to address the required or warning questions prior to completing or signing a document.

- **User is allowed to document:** When set to Allow, the user has access to the **Entry Mode** and **Document Search** options on the action bar within Documentation. It also allows access to the Document and Report folders within the document tree.

- **User is allowed to complete documents:** When set to Allow, the user has access to the **Complete** option on the action bar within Documentation.

- **Web Client Documentation**: This option allows the user to access the Documentation application from within Web Client instead of launching it via TUX.

***NOTE**: If only the Documentation application is added to a login, without specific behaviors added, Documentation displays in View Only mode.*

12.15 Electronic Signature

- **No Cosignature Needed**: When set to Allow, the user will have the ability to choose whether or not the document, document report or admission orders will require a Cosignature. The Electronic Signature page will have a new check box available for **No Cosignature Needed** during the electronic signature process. Once selected, the available Cosigners will not be available. This behavior will only work when a cosigner is connected with the Event **Patient Document Signed** or **Admission Order Signed**.

- **Remember Passphrase:** When set to Allow, the passphrase may be entered once during an electronic signature session. Once the passphrase is entered, the system will hold the passphrase for up to 24 hours. The default is one hour when the Remember Passphrase is added but additional time may be added from the Roles Settings by Facility or Login Settings by Facility.

12.16 Enterprise Wide Scheduling

- **Add and Remove Instructions:** When set to Allow, this will allow the user to add or remove scheduler or patient instructions from the patient's Event Screen or the Appointment Detail screen.

- **Delete Scheduling Image:** When set to Allow, this will enable the Delete option on the Appointment Images screen. A user may then mark an image as deleted and be able to view the image as needed.

- **Create Appointments:** When set to Allow, this will allow the user to create appointments from various places in the Updated Scheduling application. This will give them access to the following screens: Patient Appointments, Wait List, Grid Views, Appointment Detail, Event Screen, Group Detail

- **Create/Edit Blocks:** When to Allow, this will enable the Block option of the day/week views on the action bar.

- **Create/Edit My Schedules:** When set to Allow, this will allow the user or role to create schedules and make changes to an existing schedule created by them. When set to Deny, this will allow the users to only be able to add existing schedules, remove schedules and change the order of the schedules in the Schedule Options screen.

- **Edit Other User's Schedules:** When set to Allow, any schedule may be edited and may also be deleted. Schedules may be deleted even if the schedule is being utilized by one or more user logins; a message appears when this is the case to inform the user and allows them to cancel or proceed.
- **Open Charts:** When set to Allow, this will allow a patient's chart to be opened from the schedule.
- **Overbook Appointments:** When set to Allow, this will allow the scheduler to override/overbook appointments that have been maxed out.
- **Override Scheduling Blocks:** When set to Allow, this will allow a patient to be scheduled where a date and time have been blocked off.
- **Reassign Appointments**: When set to Allow, this will allow the user access to the Reassign option on the Day View screen when reassigning appointments to a different location, or to a different date.
- **Update Patient Email to Profile:** When set to Allow, this will allow the user to access the Patient Email field on the Event screen to either add or update the field.

12.17 Filter Builder

- **Create new filters**: When set to Allow, the user is authorized to create new filters.
- **Edit existing filters**: When set to Allow, the user is authorized to edit existing filters.
- **Modify preferences**: When set to Allow, the user has the ability to add a preference to any Login.
- **Modify value of a preference (checked, unchecked)**: When set to Allow, the user has the ability to change the default value of the preference.

12.18 Future Order

- **Access All Future Orders:** The Release Future Orders behavior control is a prerequisite for this application. When set to Allow, and future orders from multiple departments are present, this will allow users to have access to view all future orders from all departments, but they will only have access to release future orders that pertain to their respective department. When set to Deny, only future orders pertaining to their respective department will display.
- **Release Future Orders:** When set to Allow, and there are future orders to be released, the **Future Orders** option is enabled on all ancillary patient function screens providing access to the Unreleased Future Orders screen. When set to Deny, the Future Orders option is disabled.
- **Require Order Reason for Future Orders:** When set to Allow, users are required to address the Order Reason before updating/signing a Future Order.

12.19 Health Information Resource

- **Access Portal Customer Support Admin Tool:** When set to allow, the Launch CSA option is enabled to allow the user to access the CSA Tool for MyCareCorner. When set to Deny, the Launch CSA option will not display within the action bar of the Portal Management screen.

- **Allow Deleting Documents**: When set to Allow, the **Delete** option is enabled when selecting a patient's CCDA from the Document View screen within the Document Queue List. When set to Deny, the Delete option is disabled.

- **Allow Importing Documents**: When set to Allow, the **Import** option is enabled when selecting a patient's CCDA from Document View screen within the Document Queue List. When set to Deny, the Import option is disabled.

12.20 Help

- **Access Learning Management System:** When set to allow, users will have access to the Help option in Thrive. This will then allow users to access CPSIQ directly.

12.21 InfoButton

- **View More Information**: When set to Allow, this will allow access to the **More Info** and **Dose Info** options where available within all applications the user login may access. These options exist in the CPOE, Medication Reconciliation, Problem List, Order Chron, Home Screen, Alerts and ChartLink applications.

12.22 Information Submission

- **Link and Retitle Information Submissions**: When set to allow, the user will have access to the Import option within Information Submissions and will also be able to select a document title for the document that is being imported into a visit.

12.23 Interface

The Interface behavior controls vary for each facility depending on the interface being used. Please contact a TruBridge Interface representative for questions regarding these behaviors.

12.24 Laboratory

- **Report Pathology Cancer Cases:** When set to "Allow" users may select the "Reportable" option in the Pathology application and send electronically signed positive cancer cases to the state registry. When set to "Deny" the "Reportable" option in the Pathology application will be disabled.

12.25 MAR

- **Administer Class 1 Or 2 Substances:** When set to Allow, the user has the ability to administer DEA Class 1-2 controlled substances.
- **Administer Class 3 Thru 5 Substances:** When set to Allow, the user has the ability to administer DEA Class 3-5 controlled substances.
- **Administer Medications:** When set to Allow, the user has the ability to administer, omit or discontinue a medication via the MAR or Med-Verify. The ability to document a reaction/response to a medication administration is controlled by this setting. Controlled substance and insulin administrations are not included in this option.
- **Amend MAR Documentation for Any Login:** When set to Allow, the user has the ability to super amend another user's documentation in EMAR.
- **Be Second Witness:** When set to Allow, the user has the ability to witness a medication administration if required by item setup.
- **Change Diabetic Record:** When set to Allow, the user has the ability to modify a Diabetic Record protocol.
- **Change PCA Protocol:** When set to Allow, the user has the ability to modify a PCA protocol.

12.26 Medical Necessity

- **Prompt for Medical Necessity Check**: When set to allow, the user will be will prompted for Medical Necessity via Order Entry
- **Review Medical Necessity**: When set to allow, will display the selection of a Coverage that is on the account if it's in the contractor table. Once selected, the user will then have the ability to select either Orders, Charges, or Grouper Procedures (Medical Records Grouper) in order to run Medical Necessity checks against to determine Medical Necessity.

12.27 Medication Reconciliation

- **By-pass Alternate Med Screen for Formulary Matching:** When set to Allow, Thrive bypasses the Alternative Medication Selection screen when selecting **Continue Home** and **Reconcile** during Admission Medication Reconciliation. Order Entry will launch automatically to the item that has been set up in the Formulary Matching table.

- **By-pass Alternative Med Screen for Non-Formulary Medications:** When set to Allow, Thrive bypasses the Alternative Medication Selection screen when selecting **Continue Home** and **Reconcile** during Admission Medication Reconciliation for non-formulary medications. Order Entry will launch automatically to the item linked to formulary alternamives in the Formulary Matching table for non-formulary medications.

- **Formulary Matching:** When set to Allow, the 'Formulary Matching' and 'Matching Complete' options (when visible) shall be enabled. 'Formulary Matching' will default to Allow for the Pharmacy role (pharmcst) only.

- **Perform Medication Reconciliation to Order Entry:** When set to Allow, the user has the ability to perform an Admission Medication Reconciliation. If set to allow for a nurse user login, the nurse would be able to perform an Admission Medication Reconciliation.

- **Re-Admit:** When set to Allow, the user will have access to the Re-Admit option within Medication Reconciliation. The Re-Admit option will allow users to reverse a discharge reconciliation.

- **Ready for Pharmacy:** When set to Allow, users will have access to the Ready for Pharmacy option in Medication Reconciliation. This option will allow home medications to be matched to formulary medications before a physician performs an admission reconciliation.

- **Remove multiple home medications:** When set to Allow, the user has the ability to select multiple home medications and remove these medications from the Home Meds list within Medication Reconciliation.

- **Select All for Admission destination:** When set to Allow, the user has the ability to use the Select All Home checkbox and the Select All Active checkbox when an Admission destination type is selected.

- **Select All for Discharge destination:** When set to Allow, the user has the ability to use the Select All Home checkbox and the Select All Active checkbox when a Discharge destination type is selected.

- **Select All for Level of Care destination:** When set to Allow, the user has the ability to use the Select All Home checkbox and the Select All Active checkbox when a Level of Care destination type is selected.

- **State PMP Controlled Substance Query:** When set to Allow, the user has the ability to query the state for PMP controlled substances.

12.28 Notes

- **Access to Custom and Canned Filters:** Allows access to the Thrive Default filters within the Create Note panel and allows the ability to set up custom filters. If a user has this behavior control set to allow, they will not need the Access to canned filters behavior control.
- **Access to Notes Admin Tool:** Allows access to the Notes Admin option within Table Maintenance.
- **Access to Canned Filters:** Allows the ability to view and access the Thrive Default filters within the Create Note panel. This will display all filters within the Create Note panel except for the Chief Complaint filter and Notes CCDA Text Field filter.
- **Add and Update Chief Complaint**: When set to allow, the Chief Complaint filter will display within the Create Note panel and allows the user to be able to pull the Chief Complaint from Thrive into Notes.
- **Add/Edit/Remove Allergy**: Currently in development for use within Patient Data Console.
- **Add/Edit/Remove Problems**: When set to allow, the user has the ability to enter, edit or archive historic problems within the Problem Management card of Patient Data Console.
- **Add, Edit, and Remove Surgery**: When set to allow, the user is able to add, edit and remove any previously documented surgical history and procedures from the Surgical History filter within Notes.
- **Allow No Cosignature Required Option:** Allows the option 'No Cosigner' to display within the Cosigner list in the Create Note Panel. If set to deny, the 'No Cosigner' option will not display within the cosigner drop down listing.
- **Chief Complaint Read Only:** Allows the user to have view only access to the Chief Complaint filter within Notes and the card within Patient Data Console. From the Notes application, the plus icon in the Chief Complaint filter will not display only allowing the user to insert the filter into the Create Note panel. From Patient Data Console, the user will not be able to enter or edit any data within the chief complaint card.
- **Copy Forward Notes**: When set to allow, the user is able to copy forward signed notes.
- **Edit other people's draft note**: When set to allow, the user is able to edit unsigned notes that are created by another user.
- **Edit other people's signed Notes**: When set to allow, the user is able to edit other user's signed notes.
- **Edit own signed Notes**: When set to allow, the user is able to edit their own signed notes.
- **Enter Historic/Resolved Problems**: When set to allow, the user has the ability to enter and edit historic problems within the Problem Management card of Patient Data Console. This also denies the ability to archive a historic problem.

- **Import CPSI Notes Templates:** TruBridge Use Only.
- **Mark Other People's Signed Note Erroneous:** Allows a user to mark another user's signed note erroneous.
- **Notes CCDA Text Field**: When set to allow, the user has access to all options within the Medical Summary Field filter:
  o Assessment
  o Hospital Course
  o Plan
- **Note Creation Access**: When set to allow, the user is able to select Create Note to start the process of creating a note on a patient account.
- **Note Viewing Access**: When set to allow, the user is able to view notes available within the Note List panel.
- **Phrase Search/Insert Access**: When set to allow, the user will be able to insert and search the phrases from the Create Note panel.
- **Phrases Administrator Access**: When set to allow, the user will have access to view, create, edit existing and delete phrases for all users.
- **Phrases Creator Access**: When set to allow, the user will have access to the Create option to view published phrases, view unpublished phrases created by the logged in user, edit phrases created by the logged in user and delete phrases created by the logged in user.
- **Phrases Library Access**: When set to allow, the user will have access to the Phrase Library to view the phrases grid, search list, favorite, unfavorite and use/insert note phrases in a note only for published phrases on the Create and Edit Note panels.
- **Problems Read Only**: When set to allow, the user has view only access to the Problem Management card within Patient Data Console. This also denies the ability to archive or restore and archived problem.
- **Surgery Read Only:** Allows the user to have view only access to the Surgery History filter within Notes and the Procedure card within Patient Data Console. From the Notes application, the plus icon in the Surgery History filter will not display only allowing the user to insert the filter into the Create Note panel. From Patient Data Console, the user will not be able to enter or edit any data within the Procedure card.
- **Template Administrator Access**: When set to allow, the user may view, create, use and delete templates.
- **Template Creator Access**: When set to allow, the user may view, create and use templates.
- **Template Library Access**: When set to allow, the user may view and use templates.
- **View and Add Data Filters Access**: When set to allow, provides access to view and access filters within the Create Note panel.

- **View other people's draft note**: When set to allow, the user is able to only view other user's unsigned notes.

12.29 Order Entry

- **Ability to edit Receive Information on Hospital Ancillary Orders**: When set to Allow, this allows users to edit Receive Information on hospital ancillary orders.
- **Access Associated Problem**: When set to Allow, this allows users to access the patient's Problem List via the Associated Problem option on the Order Entry Maintenance Screen.
- **Auto-Verify Nursing Orders:** When set to Allow, enables nursing orders to be automatically verified when created by the user. When set to Deny, Nursing orders will not auto-verify. The user must verify the Nursing Order from within the current MedAct or via the Hospital Base Menu in a Nursing department.
- **Bypass Discontinued NDC Warning**: Allows the user to bypass the Clinical Monitoring screens for viewing Discontinued NDC Warning.
- **Bypass Disease Interaction Checking**: Allows the user to bypass the Clinical Monitoring screens for viewing Disease Interaction Checking.
- **Bypass Duplicate Therapy Checking**: Allows the user to bypass the Clinical Monitoring screens for viewing Duplicate Therapy Checking.
- **Bypass Food Interaction Checking**: Allows the user to bypass the Clinical Monitoring screens for viewing Food Interaction Checking
- **Bypass General Precaution Checking**: Allows the user to bypass the Clinical Monitoring screens for viewing General Precaution Checking.
- **Bypass IV Compatibility Checking**: Allows the user to bypass the Clinical Monitoring screens for viewing IV Compatibility Checking.
- **Bypass Missing NDC Warning**: Allows the user to bypass the Clinical Monitoring screens for viewing Missing NDC Warning.
- **Bypass Patient Specific Dosing**: Allows the user to bypass the Clinical Monitoring screens for viewing Patient Specific Dosing.
- **Bypass Reference Range Checks**: Allows the user to bypass the Clinical Monitoring screens for viewing Reference Range Checking.
- **Bypass Unknown NDC Warning**: Allows the user to bypass the Clinical Monitoring screens for viewing Unknown NDC Warning.
- **Collect/Receive Ancillary Orders**: When set to Allow, the **Collect/Receive** option is enabled from within Order Chronology Menu and Ancillary Order Detail Screen. When set to Deny, the **Collect/Receive** option is disabled from within Order Chronology Menu and Ancillary Order Detail Screen.

- **Discontinue Series for Ancillary Orders:** When set to Allow, the user has the ability to cancel frequency orders.
- **Link Orders**: When set to Allow, the user has the ability to link order(s) within Order Entry.
- **Modify Pharmacy Orders**: When set to Allow, this allows providers to make changes to a patient's existing pharmacy (medication) orders from the Order Chronology application.
- **Place Protocol Ancillary Orders:** When set to Allow, the user has the ability to place protocol ancillary orders.
- **Place Protocol Medication Orders:** When set to Allow, the user has the ability to place protocol medication orders.
- **Place Protocol Nursing Orders:** When set to Allow, the user has the ability to place protocol nursing orders.
- **Place Standard Nursing Orders:** When set to Allow, the user has the ability to place standard nursing orders.
- **Place Telephone Ancillary Orders:** When set to Allow, the user has the ability to place telephone ancillary orders.
- **Place Telephone Medication Orders:** When set to Allow, the user has the ability to place telephone medication orders.
- **Place Telephone Nursing Orders:** When set to Allow, the user has the ability to place telephone nursing orders.
- **Place Verbal Ancillary Orders:** When set to Allow, the user has the ability to place verbal ancillary orders.
- **Place Verbal Medication Orders:** When set to Allow, the user has the ability to place verbal medication orders.
- **Place Verbal Nursing Orders:** When set to Allow, the user has the ability to place verbal nursing orders.
- **Place Written Ancillary Orders:** When set to Allow, the user has the ability to place written ancillary orders.
- **Place Written Medication Orders:** When set to Allow, the user has the ability to place written medication orders.
- **Place Written Nursing Orders:** When set to Allow, the user has the ability to place written nursing orders.
- **Redirect Orders**: When set to Allow, the user has the ability to redirect Verbal and Phone orders. When set to Deny, the **Redirect** option will not display on the action bar.

- **Remember Co-signer for 12 Hours**: When set to Allow, the physician or physician group selected the first time the mid-level signs an order will retain the selected co-signer for 12 hours. After 12 hours the system will default back to the original settings.

- **Require Co-signer**: When set to Allow, the user will be required to have a cosigner for Order Entry. If there is no default cosigner, the user will receive a drop-down to select a physician or physician group.

- **Save Orders to Order Lists:** When set to allow, this will allow providers to save orders to Order Lists from within the Order Entry application.

- **Sign Orders:** When set to Allow, the user will have access to the **Sign Selected Orders** option when processing Hospital Orders from within Thrive Provider EHR. When set to Deny, the **Process Selected Orders** option will display when processing Hospital Orders from within Thrive Provider EHR.

- **Update Problem List from Order Entry**: When set to Allow, this allows the patient's Problem List to be updated when users associate a new problem with an ancillary order via the Associated Problem option on the Order Entry Maintenance Screen.

- **Verify Orders**: When set to Allow, the action bar option will be enabled on the main Verify Orders screen and the Order Detail screen.

- **Verify Orders on Confidential Patients**: When set to Allow, the action bar option will be enabled on the main Verify Orders screen and Order Detail screen on Confidential Patients. *(must also have Verify Orders control set to Allow)*

- **Verify Your Own Orders:** When set to Allow, the action bar option will be enabled for the user to verify orders entered via their login. *(must also have Verify Orders control set to Allow)*

12.30 Patient Data Console

- **Add/Edit/Remove Vitals:** When set to allow, access is given to add, edit and remove vitals within Patient Data Console. Only vital entries made by the logged in user may be edited and deleted. When set to deny, the vitals card will not be viewable.

- **Board Administration - Full Access Add, Edit, Remove:** When set to allow, access will be given to Manage Board Groups, Push Boards to other users, and be an administrator to manage other user's boards on their behalf. When set to deny, users will not have access.

- **Board Publish:** When set to allow, access will be given to the Publish checkbox allowing the user to publish boards they have created. When set to deny, users will not have access to the Publish checkbox.

- **Vitals - View Only:** When set to allow, view only access is given to vitals within Patient Data Console. When set to deny, vitals will not be viewable.

- **Patient Chart - Verify and Unverifiable actions**: When set to allow, access will be given to perform the Verify/Unverifiable workflow. When set to deny, users will not have access.

12.31 Patient Data Console - Clinical Lens

- **Full Access to Clinical Lens Features:** When set to allow, full access will be given all Clinical Lens Features. When set to deny, no access will be given.

12.32 Phys Doc

- **Administrative Template Maintenance Privileges:** When set to Allow, this will allow users or roles to edit or delete any template in the system without having to be the user who initially created the template.

- **Edit Physician Documentation**: When set to Allow, the user will have access to the New Option within the document tree and will also have access to all document titles listed under New. Upon selecting a Title, the user will have access to all Physician Documentation features on the action bar. When set to Deny, the user will only have access to Current options within the document tree. If a note is selected from the Current option, it will display in the Narrative View.

- **View Unsigned Documents**: When set to Allow, the user will be able to view unsigned Physician Documentation notes created by another provider, under the Current area. When set to Deny, the user will not be able to view unsigned Physician Documentation notes created under another provider's name.

12.33 Plan of Care

- **Add/Edit Plan of Care**: When set to Allow, the user has the ability to edit existing care plans, add new problems to the care plan and import problems from the Physician Problem List. When set to Deny, the following buttons are unavailable to the user: Edit, New Problem and Import Problem.

12.34 Prescription Writer

- **Access SureScripts History:** When set to Allow, this will enable the ability to select the history tab and view the SureScripts history on a patient.

- **Add Prescribing Physician:** When set to Allow, this will enable the ability to select the Prescribing Physician drop-down field via Prescription Writer and select a prescribing physician.

- **Approve Prescription Refill Request:** When set to Allow, this will enable the ability to approve prescription refill requests sent through SureScripts.

- **Discontinue Prescriptions:** When set to Allow, this will enable the ability to to select the discontinue option for active prescriptions from Prescription Writer.

- **Do Prescription Entry, View, Print:** When set to Allow, this will enable the ability to create prescriptions from Prescription Writer as well as view the prescription document and print the prescription to a designated and locked printer on state-approved paper.

- **Enter No RX Needed Prescriptions Only:** When set to Allow, this will enable the ability to enter prescription information into Prescription Writer, but it will only allow for the selection of the "No Rx Needed" radio button next to Prescribing Methods. With instances dealing with reviewing an Rx that is marked as DAW/Generic Subsitution Permitted allows editing of discharge instructions and next dose field within a medication entry.

- **Fax Prescriptions:** When set to Allow, this will enable the ability to select the fax option to send prescriptions from Prescription Writer.

- **Renew Prescriptions:** When set to Allow, this will enable the ability to select the renew option for prescriptions from Prescription Writer.

- **Re-print Prescriptions:** When set to Allow, this will enable the ability to select the Re-print option from Prescription Writer.

- **Send Electronic Prescriptions:** When set to Allow, this will enable the ability to select the electronic option to send prescriptions electronically to pharmacies that use SureScripts from Prescription Writer. For a provider, the EScribe setup must also be completed via the Physicians and Physician Security tables.

Three levels of Prior Authorization Behavior Controls have been added. To see the permissions for each behavior, please review the table below.

- **Prepare Prior Authorization** - PAPreparer
- **Review Prior Authorization** - PAReviewer
- **Submit Prior Authorization** - PASubmitter - This is a default control for the physician, License Practical Nurse, Nursing Staff, and Registered Nurse roles.

Activity	Description/Notes	PAPreparer	PAReviewer	PASubmitter
View Worklist	View and select tasks that require action. **Note**: Tasks may also be filtered by the provider or patient included in the auth token.	X	X	X
View Response Details	Read-only access to all response data including answers to questions for an Open response.	X	X	X
Prepare Open Response	Answer questions on Open response.	X		X
Submit PARequest	Take the answers created from 'Prepare Open Response' and submit the PARequest message to PBM/payer.			X
Acknowledge Closed	Ends the workflow process for the associated ePA case.	X		X
Acknowledge Denial	Ends the workflow process for the associated ePA case.	X		X
Acknowledge Approval	User indicates agreement with approval restrictions (if any). Ends the workflow process for the associated ePA case.	X		X
Acknowledge Deferred	User indicates they have acknowledged that the PA has been deferred.	X		X
Create Appeal	Add information required to submit initial PAAppealRequest and submit.	X		X
Submit Appeal	Take the answers created from 'Prepare Open Response' and submit the PAAppealRequest message to PBM/payer.	X		X
Cancel Process	Submit PACancelRequest request to the PBM/payer.	X		X
Acknowledge Cancel	Ends the workflow process for the associated PA case.	X		X

Prior Authorization Levels

12.35 Problem List

- **Update Problem List:** When set to Allow, this will grant the user access to edit and update the Physician Problem List.

12.36 Quality Measures

- **Edit Quality Reporting Filter:** When set to Allow, users will have the ability to access and edit the Quality Measures Filter Control screen.

12.37 Report Scheduler

- **Ability to delete any Report Scheduler File:** When set to allow, users are able to delete generated reports from Report Scheduler.
- **Edit/Cancel Any Scheduled Report:** When set to allow, users are able to edit and cancel reports scheduled by other users.
- **Schedule Reports:** When set to allow, users are able to create scheduled reports and edit and cancel reports they have previously scheduled.
- **Send reports using SFTP:** When set to allow, users are able to export reports to the facilities SFTP server.

12.38 Resulting

- **Amend Clinic Lab Results:** When set to Allow, the user has the ability to amend clinic lab results. Clinic orders are defined when the first two numbers of the seven digit order number correspond with the clinic OE prefix in the clinic control table.
- **Amend ED Lab Results:** When set to allow, the user has the ability to amend completed ED lab results and the option for Amend will be available from the result screen. ED orders are defined when the item is added to the Resulting Items Table in ED Control Information on the Table Maintenance - Control page. The ED will use the same OE Prefix as the Lab Department.
- **Edit Clinic Lab Results:** When set to Allow, the user has the ability to enter clinic lab results. Clinic orders are defined when the first two numbers of the seven digit order number correspond with the clinic OE prefix in the clinic control table.
- **Edit ED Lab Results:** When set to Allow, the user has the ability to enter ED lab results and the options for Save and Complete/Save will be available from the result screen. ED orders are defined when the item is added to the Resulting Items Table in ED Control Information on the Table Maintenance - Control page. The ED will use the same OE Prefix as the Lab Department.

12.39 Secure Messaging

- **Create/Reply Secure Messages**: When set to allow, gives the ability to create and reply to secure messages within the Communications application. When set to deny, the ability to select the Reply, New Message and Send options are disabled.

12.40 Security

- **Create And Edit Logins:** When set to Allow, this will allow new logins to be created and existing logins to be edited for employees and physicians in System Administration. It will also allow access to the Client Version Setup Screen.
- **Modify Login and Password Policies:** When this is set to Allow, this will allow the Login and Password Policies to be changed and saved on the Security screen within System Administration.
- **Unlock And Reset Passwords:** When set to Allow, this will allow the user to unlock or reset logins for employees and physicians.

12.41 Table Maintenance

- **Create/Edit Charge Templates:** When set to Allow, the user will have the ability to add, edit and delete Charge Templates on the Control Tab in Table Maintenance. When set to Deny, the Charge Set Maintenance screen is view only.
- **Delete Performing Lab:** When set to Allow, the user will have the ability to delete an existing Performing Lab.
- **Edit Admin Groups:** When set to Allow, the user will have access to make changes to the Admin Groups table on the Control Tab in Table Maintenance.
- **Edit AR Last Cycle Run:** When set to Allow, the user will have access to change the Last Cycle Run field within the Collections Settings table.
- **Edit AR Minimum Payments:** When set to Allow, the user will have access to make changes to the AR Minimum Payments within the Collections Settings table.
- **Edit AR Statement Messages:** When set to Allow, the user will have access to the AR Statement Messages table.
- **Edit Blood Administration Application Switch:** When set to Allow, the user will have the ability to access the Blood Administration option in the Laboratory Control Options table.
- **Edit Collection Unit:** When set to Allow, the user will have access to make additions to the Unified Code for Units of Measure table.
- **Edit Department Ancillary Application Switch:** When set to Allow, the user will have access to the Ancillary Application option within the department table setup.
- **Edit Diet Switch OE Info:** When set to Allow, the user will have access to the Diet Switch field in the Item Master. When set to Deny, the field will not display.

- **Edit Item Average Cost:** When set to Allow, the user will have access to the average cost field in the Item Master.
- **Edit Item Master:** When set to Allow, the user will have the ability to edit the Item Master.
- **Edit Item Prices:** When set to Allow, the user will have the ability to edit the pricing for an item within the Item Pricing Information option in the Item Master.
- **Edit Navigation Customization:** When set to Allow, the user will have the ability to save the order of any other user login's Navigation Customization. When set to Deny, the user will only have the ability to save the order of their own Navigation Customization.
- **Edit OID Assignment:** When set to Allow, the user will have the ability to access and edit the Insurance OID Assignment table. If access has not been given, or it has been denied, this table will be read only and any options on the screen will be grayed out.
- **Edit Performing Lab:** When set to Allow, the user will have access to edit or create an existing Performing Lab.
- **Edit Specimen Tables:** When set to Allow, the user will have access to make changes to the Specimen Tables, the Observation Tables, and the Specimen Information Defaults.
- **Inactivate Vendor:** When set to Allow, the user will have the ability to inactivate a vendor in the Item Master.
- **Order List Setup:** When set to Allow, this will enable the ability to access and edit Order List setup via Table Maintenance.
- **Order Set Setup:** When set to Allow, this will enable the ability to access and edit Order Set setup via Table Maintenance.
- **Protocol Setup:** When set to Allow, this will enable the ability to access and edit Protocol Setup via Table Maintenance.
- **SFTP Setup:** When set to Allow, the user will have the ability to access the SFTP Setup table in HIM Table Maintenance. If access has not been given, or it has been denied, only the Active or All radio buttons will be available and the reset of the screen will be grayed out.

12.42 Thrive UX

- **Access to System Menu**: When set to Allow, System Menu will be present in the application drawer when logged in with Thrive UX or Web Client. When set to Deny, access is not allowed to the System Menu while using Thrive UX or Web Client.
- **Web Client System Menu:** When set to Allow, selecting System Menu when logged in to Web Client will launch the application within Web Client. When set to Deny, selecting System Menu from within Web Client will launch the Thrive UX System Menu.

Chapter 13 TruBridge Default Rules

Evident has setup default rules to help establish security settings for specific tasks. The following rules are **not** associated with any Roles by default, but may be added to a Login or Role by using Rule Management or by accessing the Screens on the Role/Login and selecting Associate Rule. These rules were intended to provide a less labor-intensive method for assigning security in System Administration.

***NOTE**: Application 68, Screen 85, and Behavior Control 76 rule defaults for each Role are listed under the Role section of this user guide.*

Default Behavior Control Rule

Default behavior control rules may be added to a Login or Role by using Rule Management or by accessing the Screens on the Role/Login and selecting Associate Rule.

- **Default Registration Behavior Control Rule**: This rule is intended to give access to the behavior controls needed to perform registration tasks within Thrive. The following behavior controls are available with this rule:
  - Edit Chief Complaint
  - Edit Consent/Privacy Notice
  - Edit Med History Consent
  - Edit Exclude from Portal
  - Edit Exclude from API
  - Edit HIE Shared Data
  - Edit Data Sensitivity Level
  - Edit Protect Immunization Data
  - Edit ER Log
  - Update Problem List
  - Edit Guarantor Note
  - Add New Guarantor Note
  - Access Learning Management System

- **Default BC Rule for Auditing Table Maintenance**: This rule provides access to audit information associated with the Table Maintenance role in the Change Log. In addition to this rule, the 'TruBridge Default Screen Rule for Auditing Table Maintenance' is also recommended. Together these rules will allow access to the Change Log for audit information associated with the Table Maintenance role. The following behavior control is available with this rule:
  - Audit access for Table Maintenance Role

Default Screen Rules

Default screen rules may be added to a Login or Role by using Rule Management or by accessing the Screens on the Role/Login and selecting Associate Rule. The following default screen rules are available:

- **Default Patient Registration Screens**: This rule is intended to provide access to the screens needed to perform registration tasks. The following screens are available with this rule:
  - Room List
  - ClinDoc Main Screen
  - Form Runner Screen

- **TruBridge Default Screen Rule for Account Detail**: This rule allows access to the Account Detail screen.
  - ar_account_detail

- **TruBridge Default Screen Rule for Auditing Table Maintenance**:This rule is intended to allow access to the security change log without disclosing other sensitive information. Behavior Controls are needed in order to view audit information in the Change Log. In addition to this rule, the 'Default BC (Behavior Control) Rule for Auditing Table Maintenance' is also recommended. Together these rules will allow access to the Change Log for audit information associated with the Table Maintenance role. The following screens are available with this rule:
  - Security Change Log
  - Security Audit Log
  - Data Dictionary Customer List

- **TruBridge Default Screen Rule for Coding**: This rule is intended to allow access to the screens needed to perform coding tasks. The following screens are available with this rule:
  - Order Chronology Nursing Detail Screen
  - Patient Demographics Selection
  - Order Chronology Screen
  - Care Plan List
  - Visit History Screen
  - Health History Base Menu
  - MAR Main Screen
  - Patient Clinical History Screen
  - Disciplines Screen
  - PACS Image Screen
  - Patient Transcriptions Screen
  - Patient Demographics - Encounter
  - Patient Allergy List Screen
  - Clinical Monitoring Review Screen
  - Add Health History Entry
  - ICD Modifiers List
  - MAR Legend Screen
  - MAR Order Detail Diabetic Record Non-Iv Screen

- **TruBridge Default Screen for Event Setup**: This rule is intended to allow non-system administrators users to setup Events within System Administration. The following screens are available with the rule:
  - Login List Screen
  - Login Edit Screen
  - Event Rule LIst for Logins
  - Rule Builder List Script Rules Screen
  - Rule Builder Script Maintenance

- **Deny Escribe Logical Access in Table Maintenance**: This rule is intended for users that have access to the Table Maintenance Application, but do not need to be allowed access to Logical Access Control (LAC) or Electronic Prescribing of Controlled Substances (EPCS). The following screens are denied with this rule:
  - Escribe Logical Access

- **Deny Table Maintenance Security Screen**: This rule is intended to deny access to Table Maintenance and System Administration screens as a setup application but still allow them to be used as resource by other applications. This rule is typically used when the role/login has access to the Table Maintenance application; together, these rule will allow the user to access screens that derive information from the Table Maintenance application, but keep the user from changing setup with the Table Maintenance application. The rule is associated to the Physician Role by default, but can be associated with other roles/logins as needed. The following screens are denied with this rule:
  - Patient Summary Tables
  - Health Information Management Table
  - Control Tables
  - Clinical Tables
  - Patient Intake Tables
  - Business Office Tables
  - Accounting Tables
  - Rule History
  - System Filter Context
  - System Management Edit Screen
  - Facility List Screen
  - Roles List Screen
  - Inactive Logins List Screen
  - Login Edit Screen
  - Login Facility Edit Screen
  - Login Application-Cod Security Rules
  - Behavior Control Rules
  - Login Data Block Rules
  - Login Screen Security Rules
  - Login Report Rules (login_rw_rulelist)
  - Login Report Rules (login_custrep_rulelist)
  - Login Filter Context List
  - BI Component Rules
  - Event Rule List for Logins
  - Database Access
  - Home Screen Folder List

Chapter 14 Multi-Factor Authentication

The following information is intended to assist Thrive EHR users in the configuration, implementation and maintenance of Multi-Factor Authentication for Web Client.

The following terms will be used throughout this section.

- **Multi-Factor Authentication (MFA)**[1]: Authentication using two or more different factors to achieve authentication. Factors may include:
  - something you know (e.g., password/PIN);
  - something you have (e.g., cryptographic identification device, token); or
  - something you are (e.g., biometric).

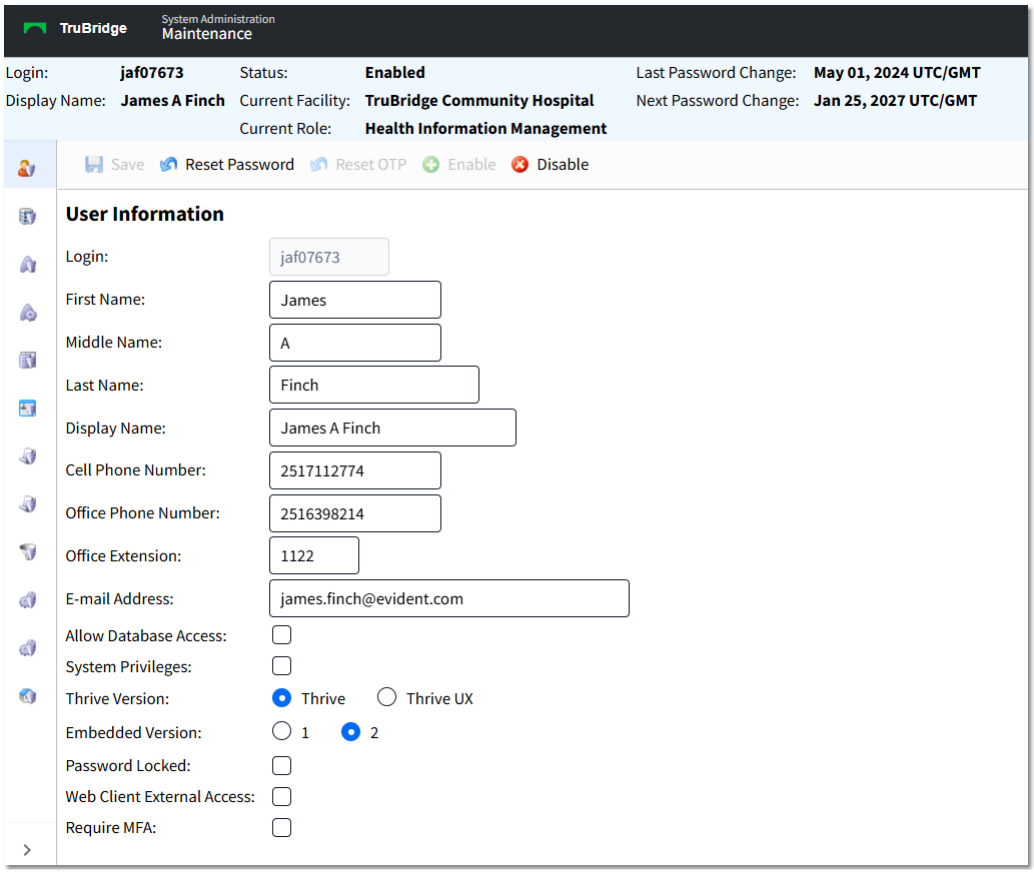
  1- *NIST Special Publication 800-53 Revision 4, April 2013*

- **One-Time Password (OTP)**: As the name suggests, this is a single-use password/token generated as the need arises. Due to only being used once, OTP may overcome many of the pitfalls of static passwords. With quick expiration, typically 30 to 60 seconds, one-time-only passwords may be simple; they do not have to meet complexity requirements.

14.1 User Login Maintenance Setup

Options are available for System Administrators to require a One-Time Password (OTP) when users access Web Client from outside the facility's network. These are found on the Maintenance screen of each login in the System Administration application.

Select **Web Client** > **System Administration** > **Logins** > **Select Login**



User Information

The two options for **Web Client External Access** and **Require MFA** are at the bottom of the screen. These options work in tandem; a user must first be authorized for out of network access for Web Client before being required for MFA.

Below is an explanation of each function.

Web Client External Access

- **Disabled (not selected)**: The user may only access the EHR via Web Client *when in the facility's network*; and is denied access when out of network.

- **Enabled (selected)**: The user may access the EHR via Web Client *when connecting both in and out of network*. If selected, the Require MFA option becomes available.

Require MFA

- **Disabled (not selected)**: An OTP is not required when accessing the EHR via Web Client *when connecting out of network*.

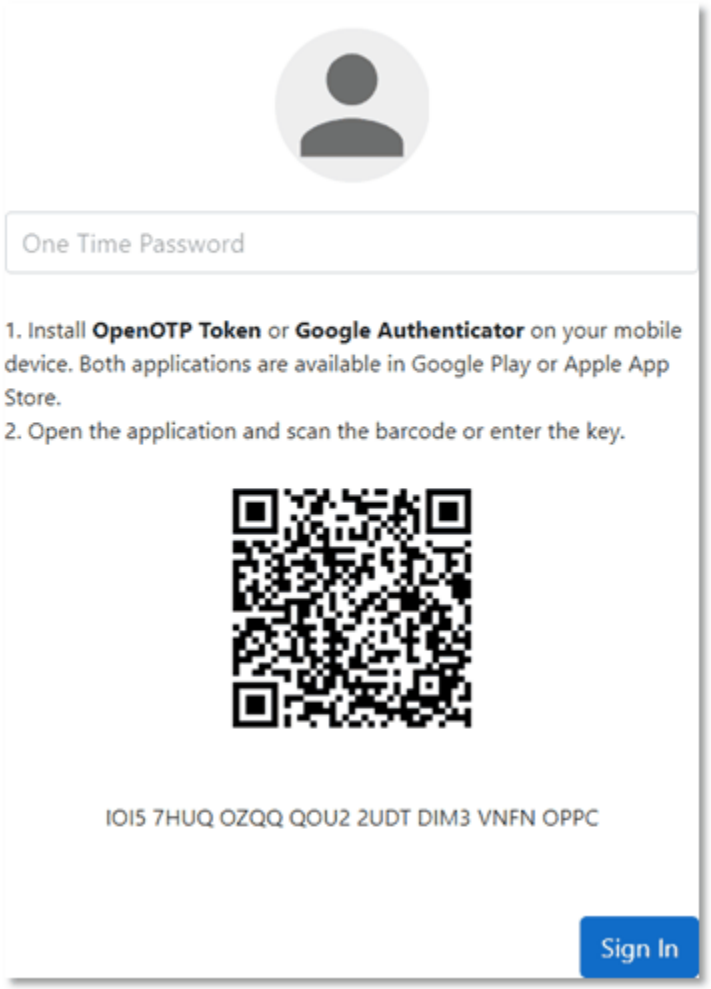
- **Enabled (selected)**: An OTP is required when accessing the EHR via Web Client *when connecting out of network*. This setting applies to out of network access only. When the same user is within the facility's network, OTP is not required.

14.2 Web Client Sign-On with MFA Enabled

TruBridge recommends using a smart phone application, such as Google Authenticator or OpenOTP, to generate a One-Time Password (OTP). Both are available for free from app stores. Once the user sets up an OTP for Web Client, the phone app generates a token that becomes the second factor for authentication.

Initial Login

When the user logs in for the first time after MFA is required, the user must first register to receive the second factor. See the screen below. The user should follow the steps on the screen to receive the first OTP password.



OpenOTP Token Registration

Once the app association to Web Client is established, the user will receive an OTP from the authenticator to type into the One-Time Password field. Once the OTP is keyed in, select **Sign In** to access the EHR.

Subsequent Web Client Logins

After the initial OTP setup is complete and the user is registered with the authenticator, subsequent logins will prompt for the OTP generated by the authenticator. There is no need to re-register.

Chapter 15 Troubleshooting

If a user accesses a screen or report and their login or role does not have a security rule setup that allows access to that application, screen or report, then the message "You are not authorized!" will display. This message will detail the unauthorized Application Code, Description, Program Name, User, Logname, Groups (role) and Facility. In this example, the user is trying to access the Aged Trial Balance report. The user is receiving this message because for one of the following reasons:

- The user or role does not have a security rule that allows access to the Accounts Receivable application.
- The user or role does have a security rule that allows access to the Accounts Receivable application, but a report security rule has been setup that denies access to the Aged Trial Balance report.
- The user or role does not have a security rule that allows access to the Aged Trial Balance report.

Unauthorized Message

If the user does need access to the screen or report, using the information provided (Application Code, Description and Program Name) will help setup the security rule.

- **Application Code**: This code may be used to identify the application that the screen or report belongs to. The application may be used to create a security rule allowing the user or role access to the entire application (all screens and reports that belong to that application).
- **Description**: This is the name of the screen or report. The screen or report name may be used to create a security rule allowing the user or role to access the specific screen or report.
- **Program Name**: The program name displays the screen's Launcher name or the report's Template name. These may be matched up to the screen or report name when creating a security rule.

There are a few options to consider when determining where access will need to be given in the Rule Builder:

- Should access be granted to the entire application, or should access only be granted to that specific screen or report.
  - If access is granted to the entire application, the user will have access to all screens and reports that belong to that application. To do this, create an application security rule that allows access to the application designated by the Application Code on the Unauthorized message.
  - If access should **NOT** be granted to the entire application, but access to the screen or report is still needed, then create a screen or report security rule that allows access to the screen or report designated by the Description/Program Name on the Unauthorized Message.

- Should access be granted to just this user, or should access be granted to everyone in the role.
  - If access should should only be granted to the user, then a security rule should be added to the login.
  - If access should be granted to all users within the role, then a security rule should be added to the role.

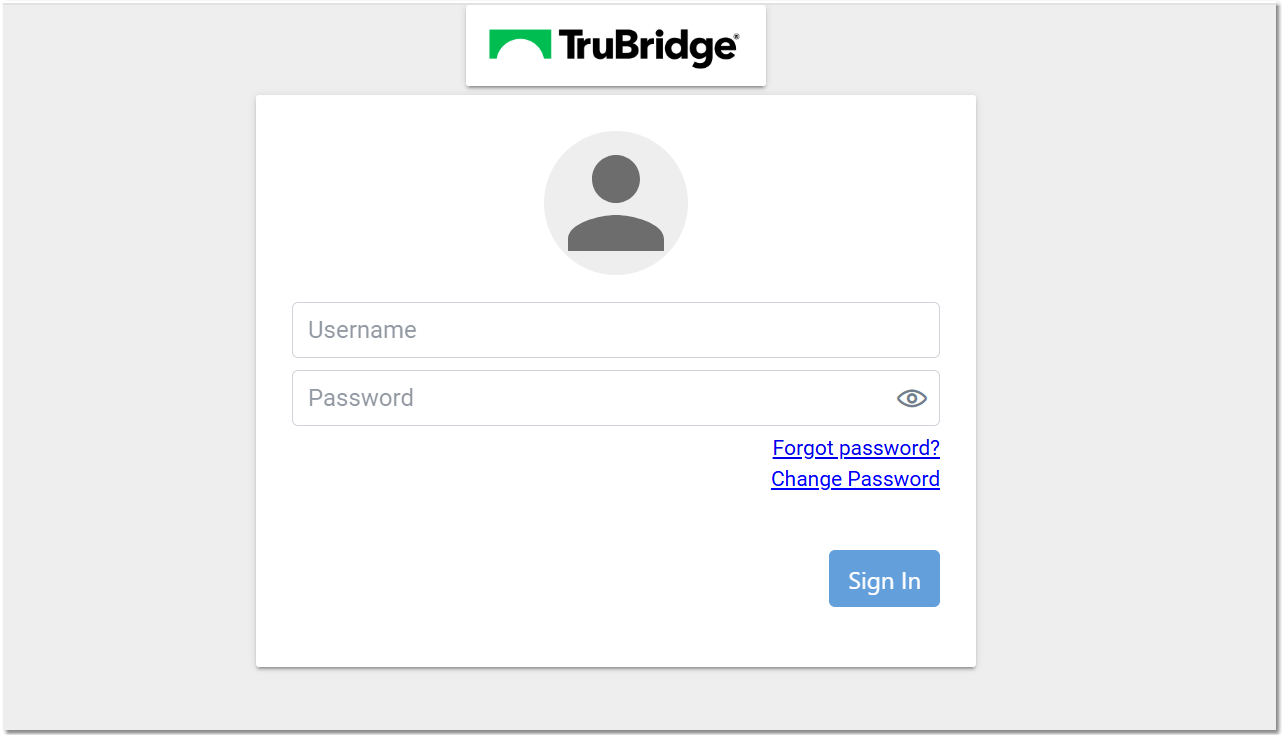
Once it has been determined if it is the user or the role that is needing access, a security rule may be added from Rule Management or from the Login or Roles screen.

Chapter 16 Logging into Web Client

Once the setup for each facility is complete, the login is ready to be used. The default password for all newly created logins is assigned by the System Administrator. This password will be used the first time a user logs in, and a prompt to enter a new password will display.

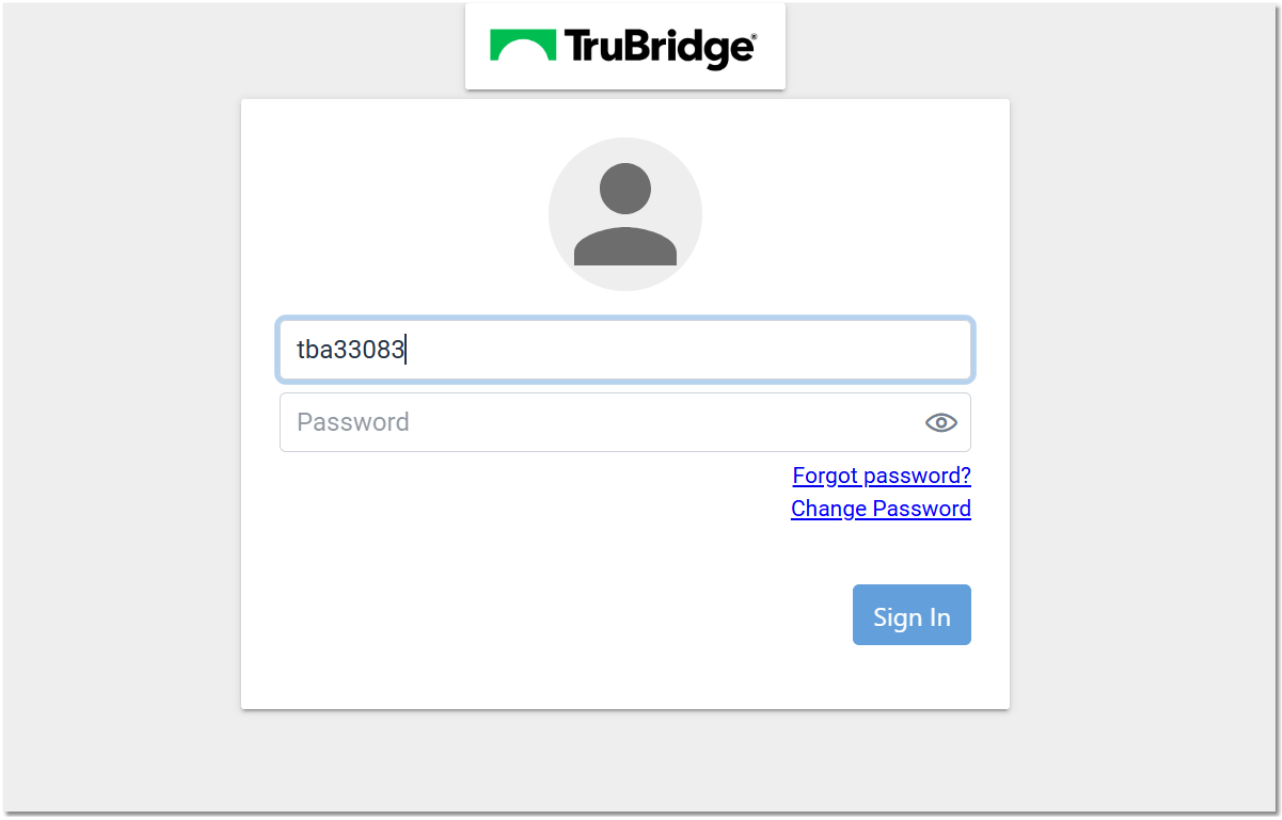
Use the following steps to log in:

1. Open Web Client



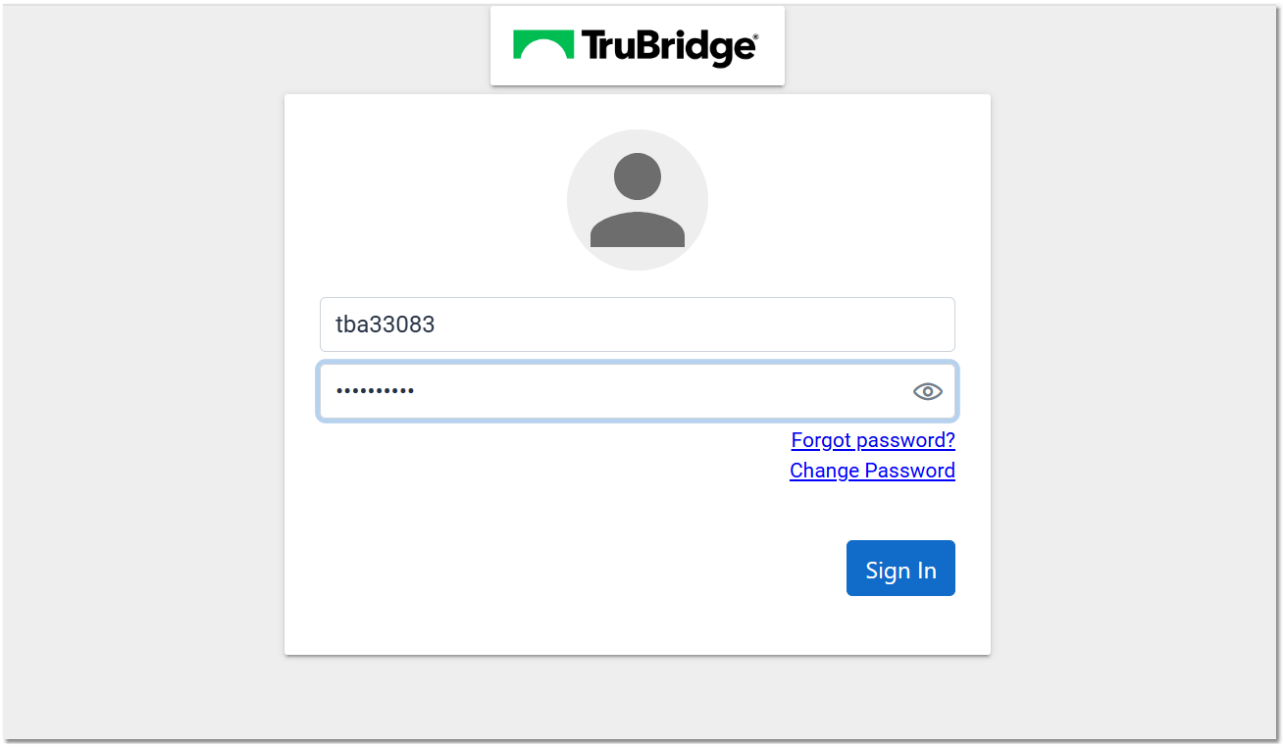
Web Client - Login

2. Enter the newly created login into the Username field.



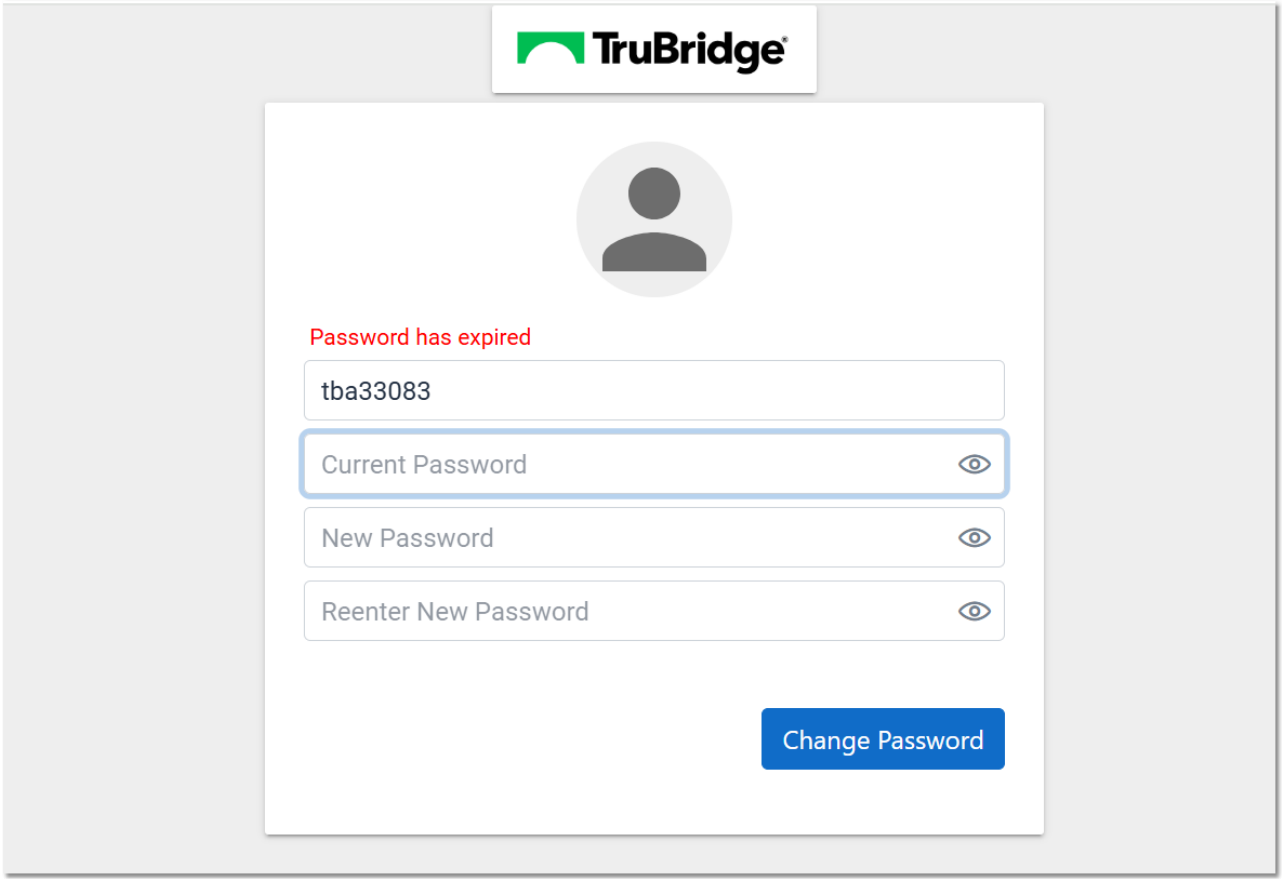
Web Client - Login

3. Enter the default password assigned by the System Administrator into the Password field and select **Sign In**.



Web Client - Login

4. Re-enter the default password assigned by the System Administrator in the Current Password field.

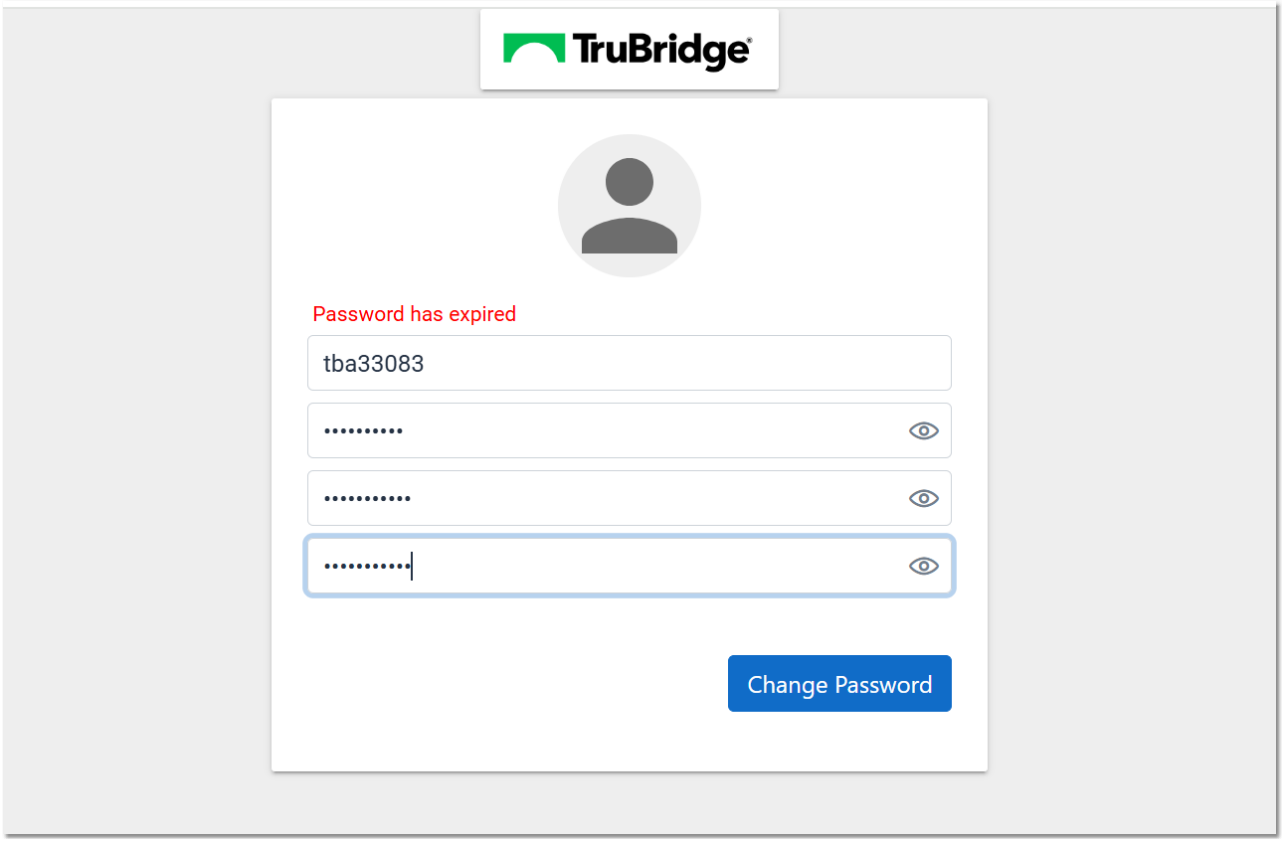


Web Client - Change Password

5. Enter the new password in the New Password field as well as the Reenter New Password field.

NOTE: *The password requirements will be different for each facility. Contact the System Administrator for information regarding facility password policies*.

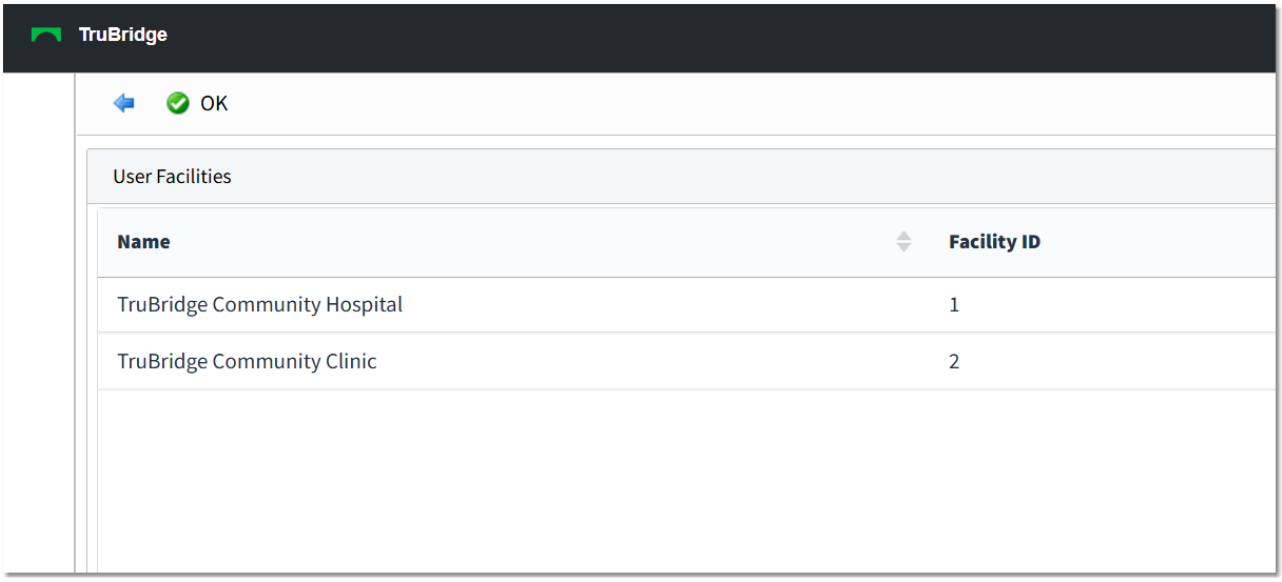
6. Select **Change Password**.



Web Client - Change Password

7. If the password meets all of the requirements and the user has access to only one facility, the user will be logged into Web Client.

8. If the user has access to multiple facilities, the user will be prompted to select a facility to log into.



User Facilities

9. From the User Facilities list, select the appropriate facility.

10. Once a user has logged into the appropriate facility, they will be logged into Web Client.

Chapter 17 Forgot Password via Web Client

17.1 Overview

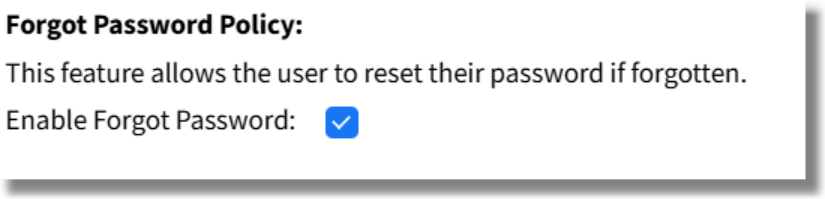
The Forgot Password feature allows users with a verified email address to reset their TruBridge EHR password directly from the Web Client login screen, without requiring administrator assistance.

17.2 Forgot Password Setup

The Forgot Password feature must be enabled before it can be used. Once it has been enabled, administrators may also choose to enable domain restrictions and customize a list of notification recipients.

Enable Forgot Password Policy

Select **Web Client** > **System Administrator** > **System**

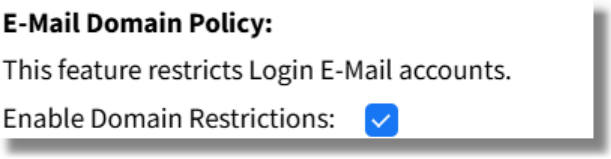


Login Policy - Forgot Password Policy

- **Enable Forgot Password:** When enabled, this feature allows users with a verified email address to reset their password directly from the Web Client login screen.

Enable Email Domain Policy

Select **Web Client** > **System Administrator** > **System**



Login Policy - Email Domain Policy

- **Enable Domain Restrictions:** When enabled, this feature allows administrators to restrict which email domains users may enter. To configure domain restrictions, select **Manage E-Mail Domains** from the action bar.

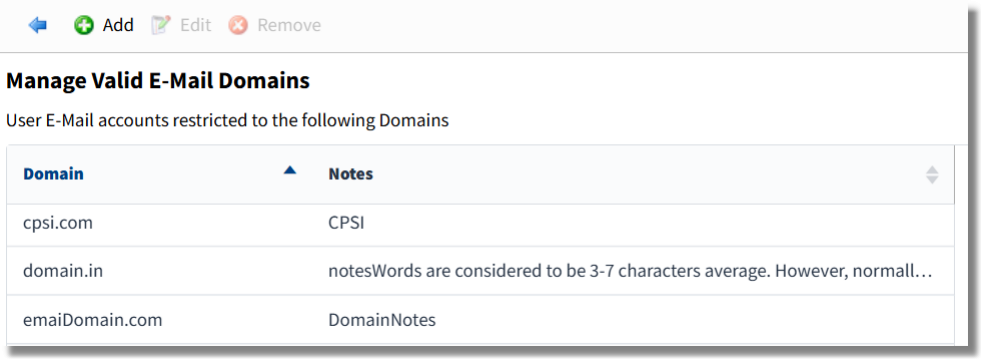
NOTE: *Domain restrictions apply only to email addresses that users enter themselves on the Profile tab under Settings. Administrators can still enter any email address on the User Information page on the Logins screen.*

Manage E-Mail Domains

To specify which domains users are allowed to use in their email addresses, restricted domains may be configured within **Manage E-Mail Domains**.

Manage E-Mail Domains

Select **Web Client** > **System Administrator** > **System** > **Manage E-Mail Domains**



Manage Valid E-Mail Domains

After selecting **Manage E-Mail Domains**, a list of existing restricted domains and any associated notes (if applicable) will be displayed.

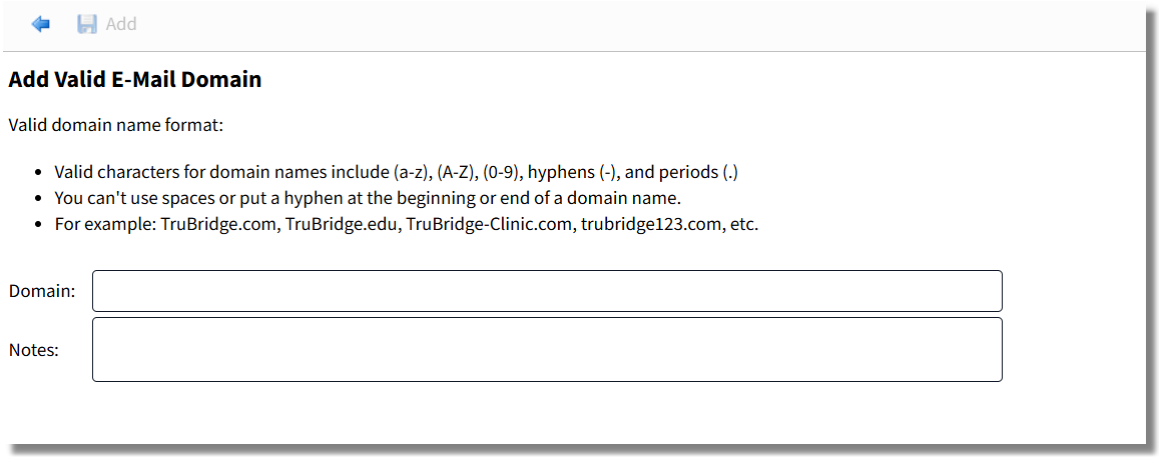
- **Add:** Allows the creation of a new restricted domain.
- **Remove:** Allows the removal of an existing domain.
- **Edit:** Allows notes to be added or updated for an existing domain.

NOTE: *Only the notes associated with existing domains may be edited. The domain name itself is not editable. To modify a domain, it must be removed and re-added with the desired value.*

Add Valid E-Mail Domain

When **Add** is selected, enter the domain name, ensuring it follows the valid format provided on the screen. Adding a note is optional.

Select **Web Client** > **System Administrator** > **System** > **Manage E-Mail Domains** > **Add**



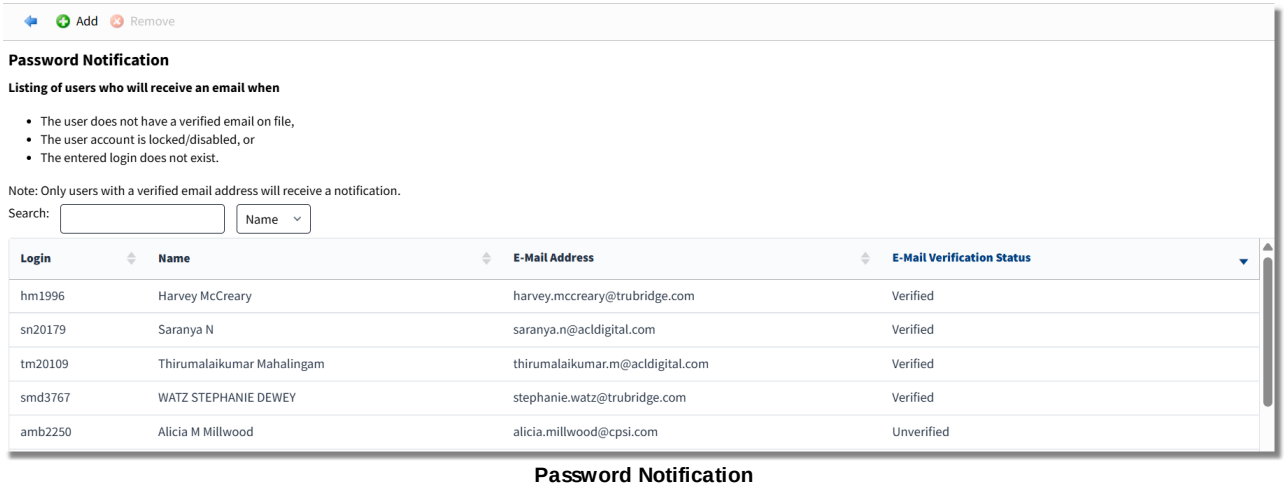
Add Valid E-Mail Domains

Password Notification List

The Password Notification List allows facilities to designate users who will receive email alerts when a password reset error event occurs. To configure the list of users, select **Password Notification** from the action bar.

Password Notification List

Select **Web Client** > **System Administrator** > **System** > **Password Notification**



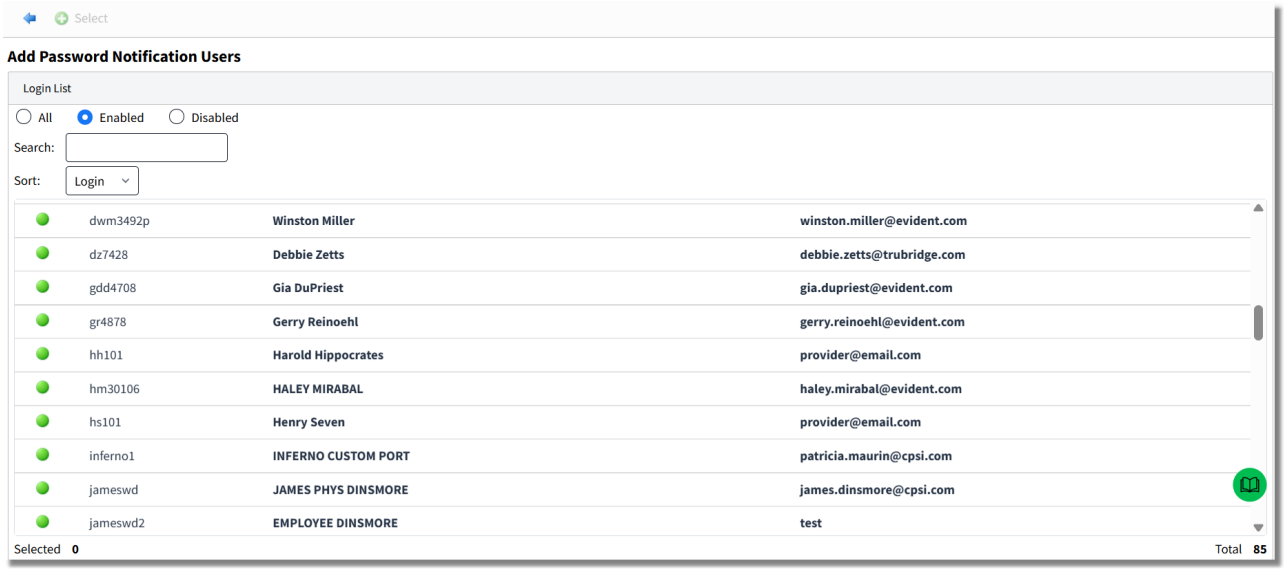
Password Notification

Users on the Password Notification List will receive an email when any of the following events occur:

- A user attempts to reset a password without a verified email address on file.
- A user account is locked.
- An invalid (non-existent) login is entered.

Add Password Notification Users

Select **Web Client > System Administrator > System > Password Notification > Add**

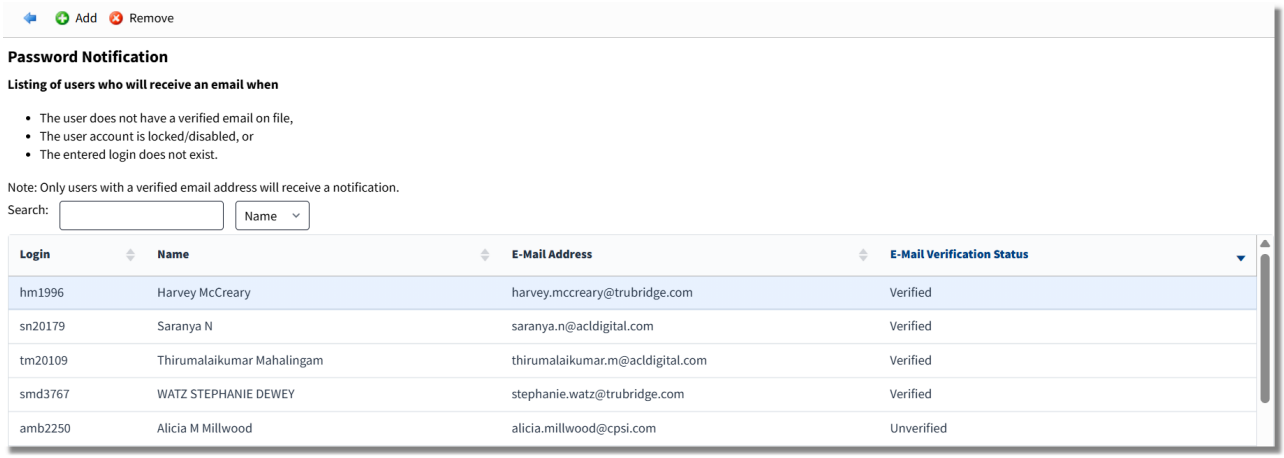


Add Password Notification Users

- To add users to the list, **double-click** the user's login from the list. The search bar may be used to find an individual user.

Remove Password Notification Users

Select **Web Client > System Administrator > System > Password Notification**



Password Notification

- To remove a user, select the user's login from the list and then select **Remove**. The search bar may be used to find an individual user.

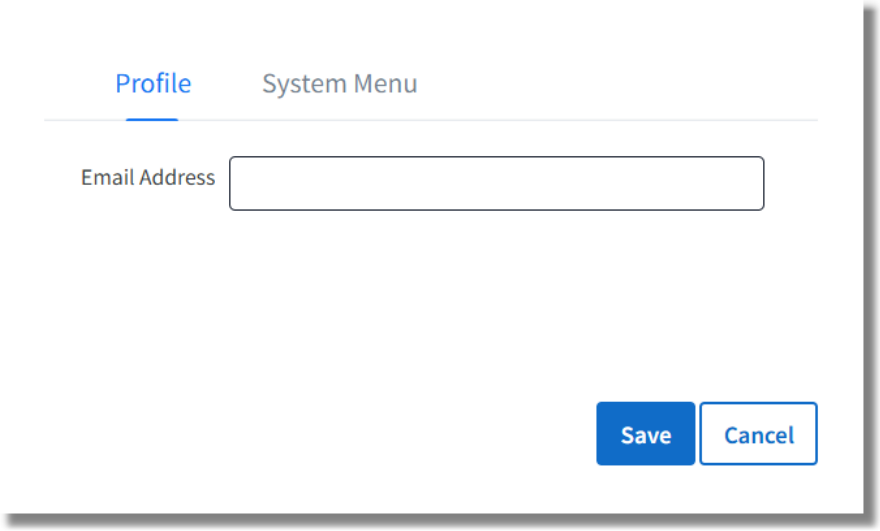
NOTE: *Users must be removed one at a time.*

17.3 Adding E-Mail Addresses

In order for users to use the Reset Password feature, their user login must have a verified email address associated with it. Email addresses may be added either by the user themselves or by System Administrators.

User-Initiated: Adding an Email Address

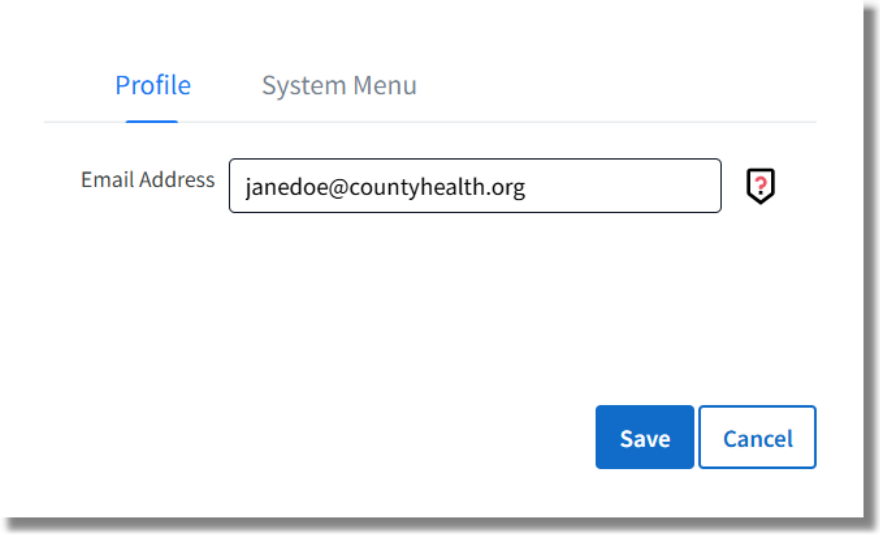
Select **Web Client** > **User Profile** > **User Initials** > **Settings**



User Profile - Settings

- From the **Profile** tab, the user should enter the email address that should be associated with their TruBridge EHR login and select **Save**. Once save is selected, a question mark icon will appear next to the address to indicate that it has not yet been verified by the user.

NOTE: *Email domain restrictions may apply, depending on system administrator settings. See* *Manage E-Mail Domains* 148 *for more information.*

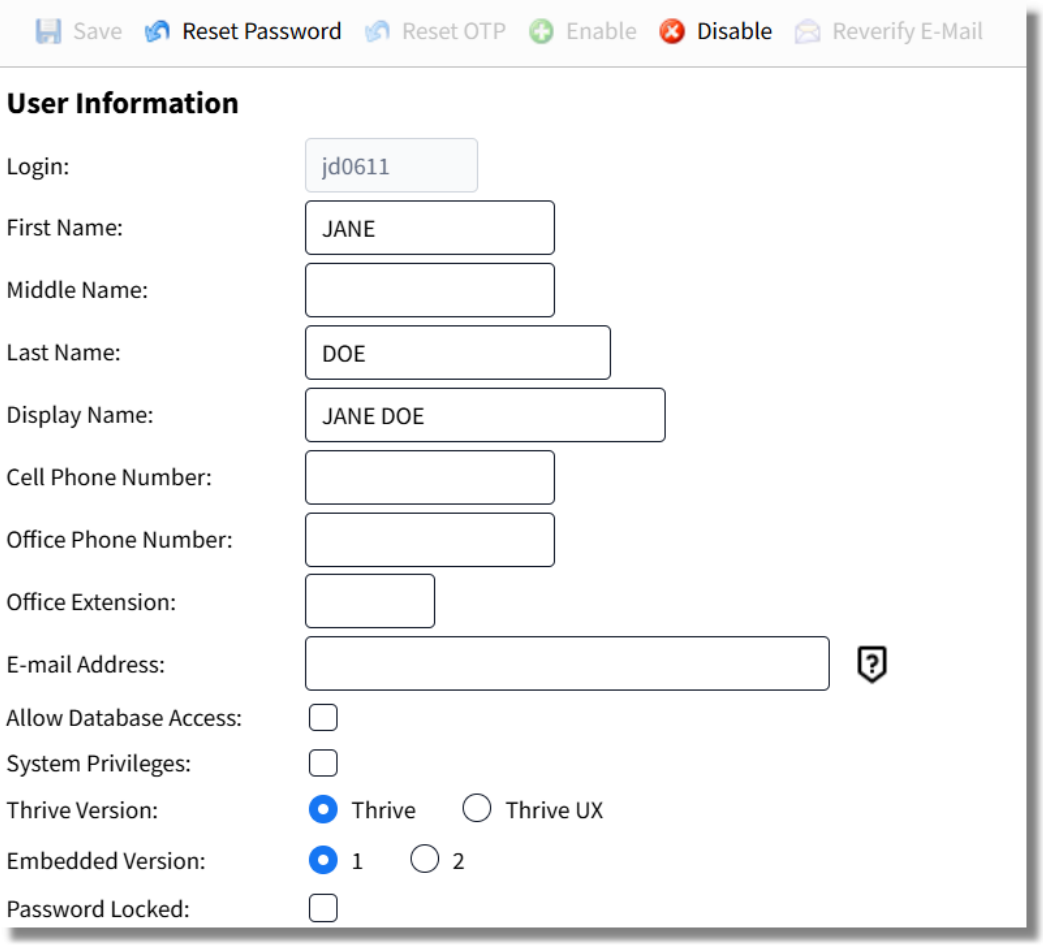


User Profile - Settings: Unverified Email Address

- Once save is selected, a verification email will be sent to the entered address. The user must verify their email to complete the verification process. See Email Address Verification 154 for more information.

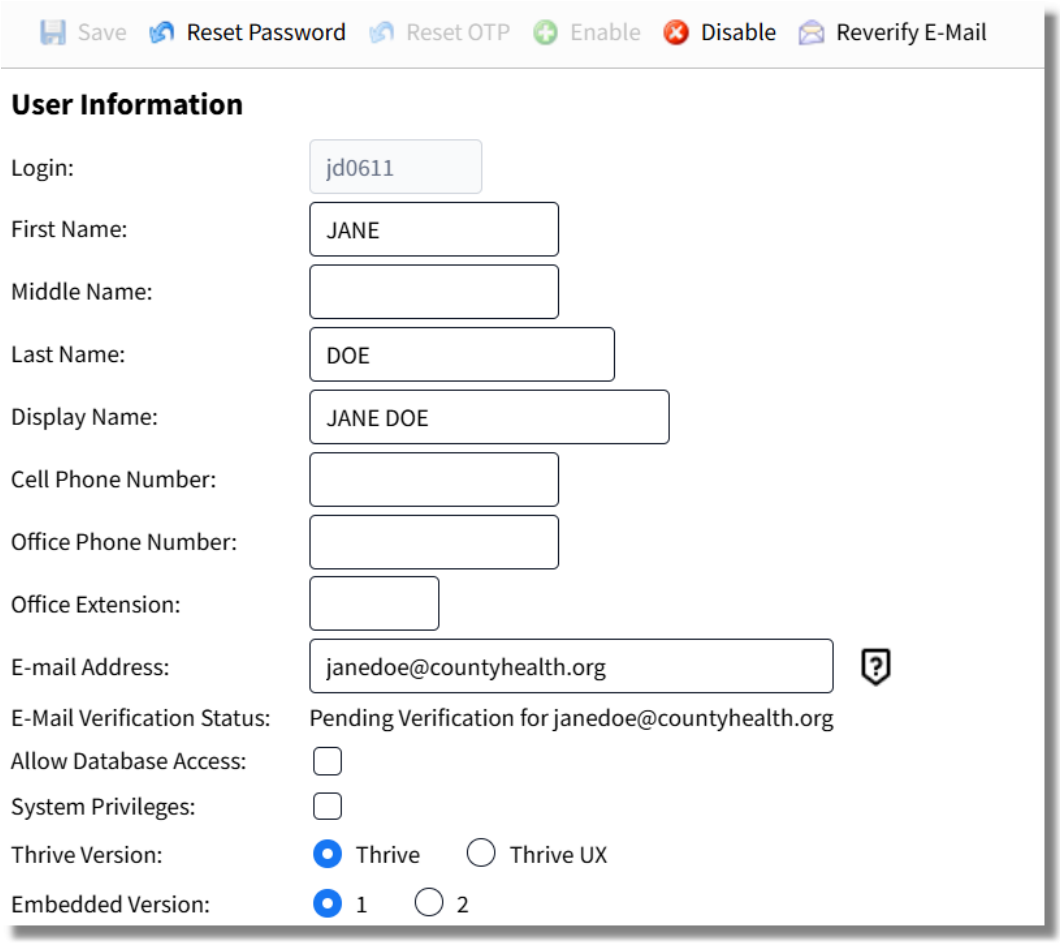
Administrator-Initiated: Add Email Address

Select **Web Client** > **System Administration** > **Logins**



System Administration - User Information

- If the **E-mail Address** field is blank, an administrator may add an email address. After entering the email address, select **Save** to begin the verification process. Once save is selected, a question mark icon will appear next to the email address. The **E-Mail Verification Status** field will also appear below it, displaying the message *"Pending Verification for [email address]"*.



System Administration - User Information: Pending Verification

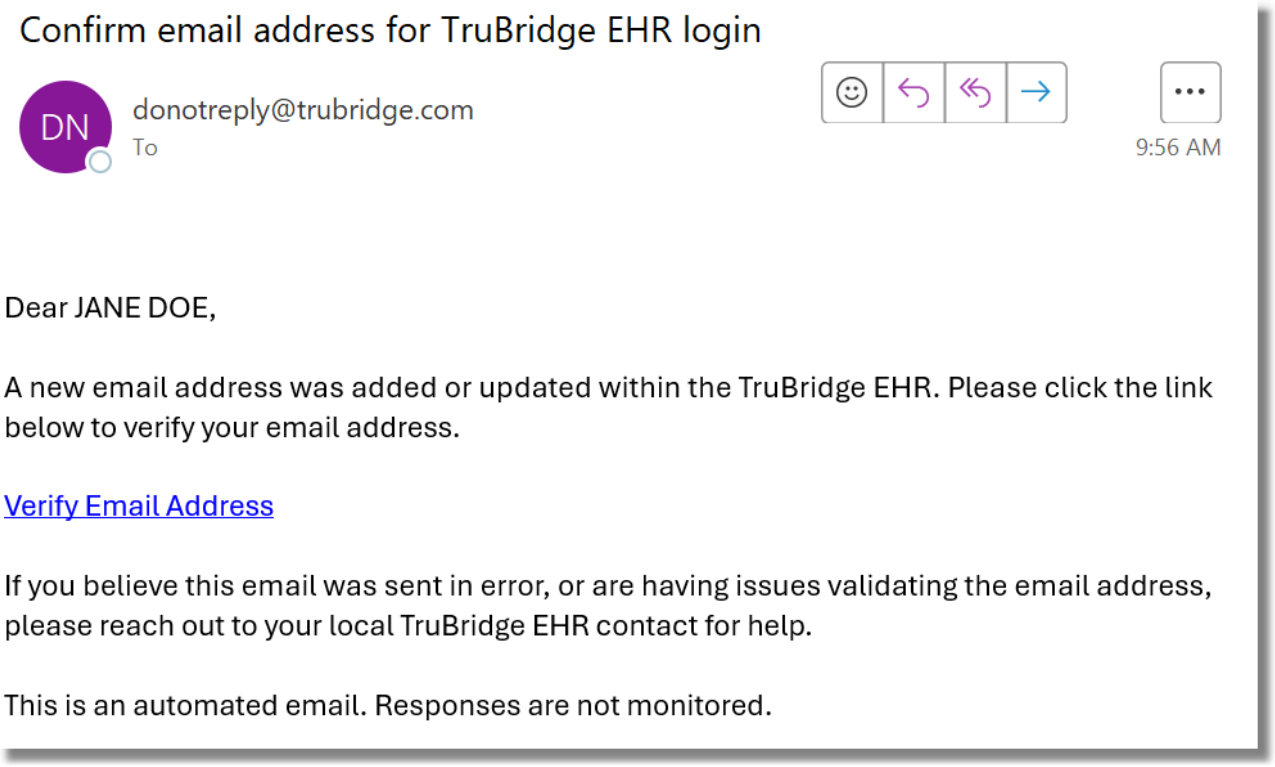
17.4 Verifying E-Mail Addresses

Once the user's email address has been entered or updated — by either the user or an administrator — a verification email will be sent to that address. The user must select the **Verify Email Address** link within the email to complete the verification process.

NOTE: *A verified email address may only be associated with one login. If the same address is used for multiple logins, only the first to complete the verification will be linked to that address.*

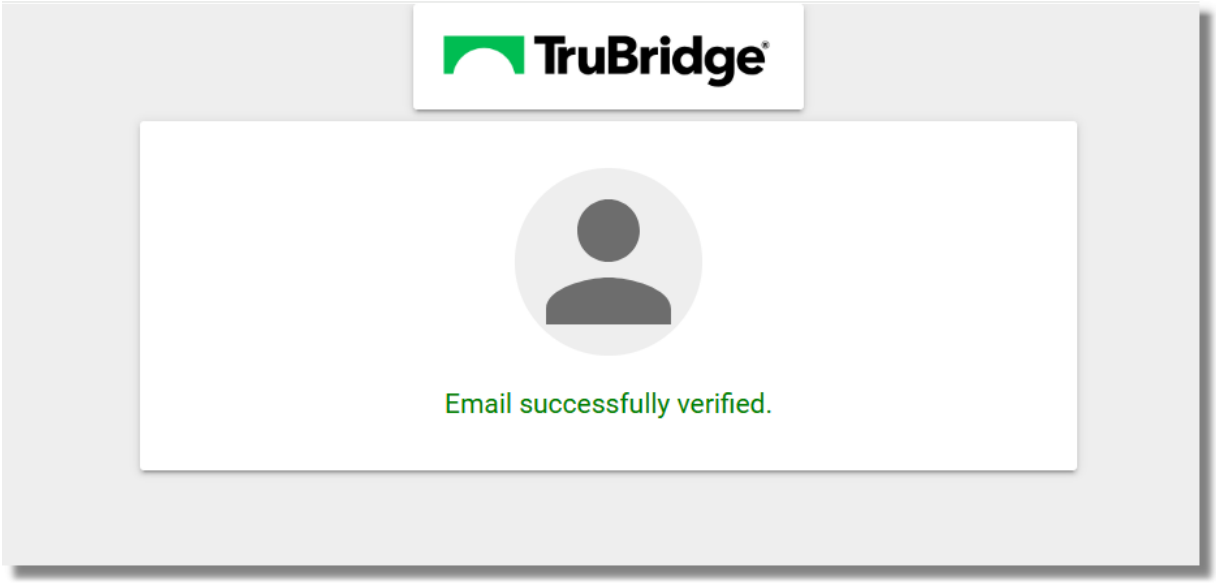
User-Initiated: Verify Email Address

- Once the user or system administrator has saved the user's email address, the user will receive an email to verify the email address. The user must then select the **Verify Email Address** link within the email.



Verification Email

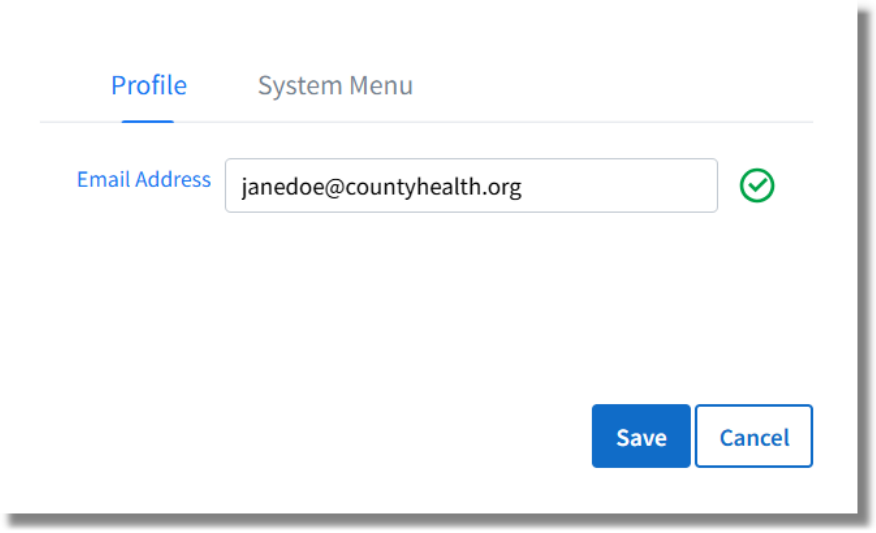
NOTE: *The verification link expires after 72 hours. If it is not used within that time, the user will need to re-enter their email address on the Profile tab and select* ***Save*** *to restart the verification process.*



Verification Email

- Once the link is selected, the user will see the **Email Successfully Verified** screen. At this point, the email address has been successfully verified.

Select **Web Client** > **User Profile** > **User Initials** > **Settings**



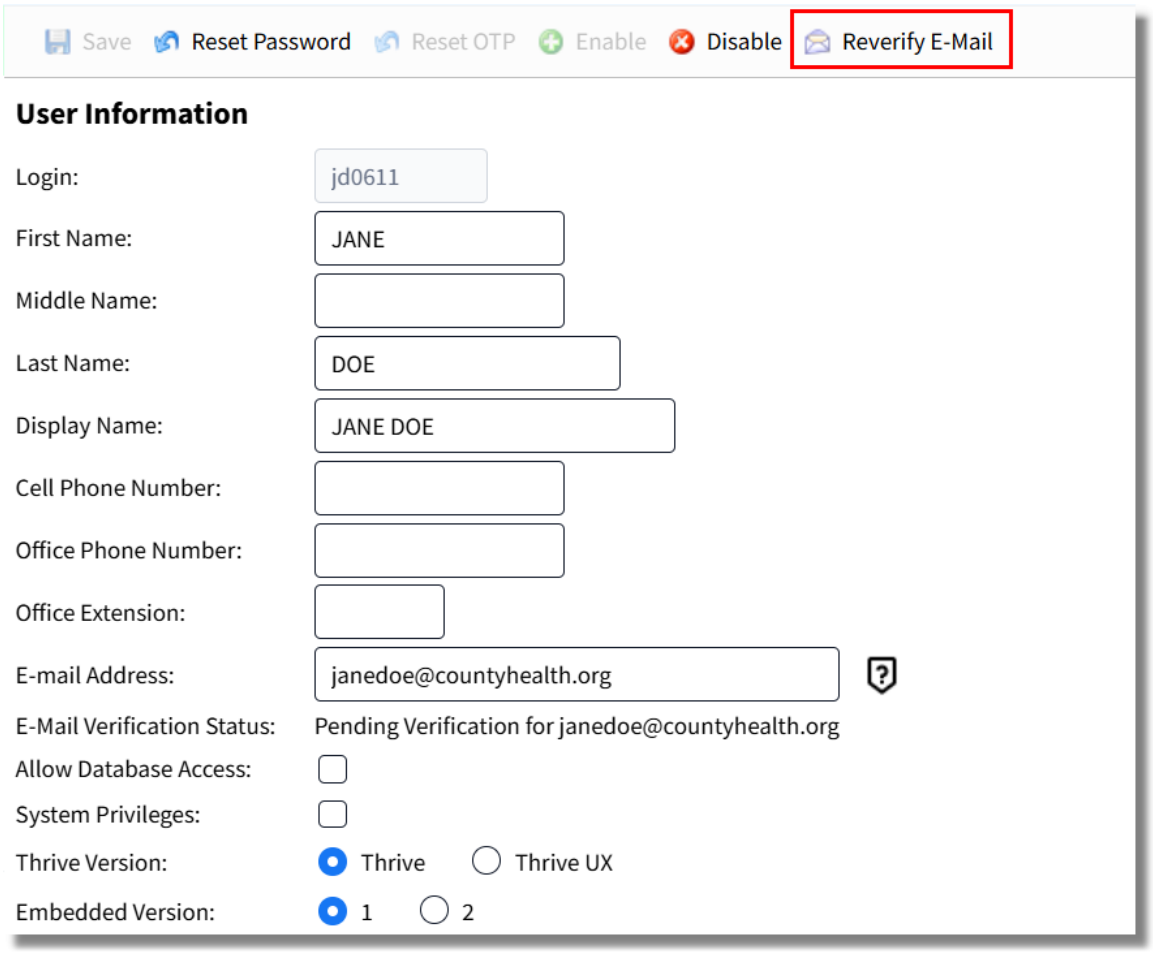
User Profile - Settings

- A **green check mark** will appear next to the user's email address on the Profile tab. The user can now use the Forgot Password feature within Web Client.

Administrator-Initiated: Manually Sending or Resending a Verification Link

- System administrators can manually send or resend the verification email to a user if needed.

Select **Web Client** > **System Administration** > **Logins**



System Administration - User Information

- To manually send or resend a verification link to a user, select the **Verify E-Mail** or **Reverify E-Mail** option from the action bar.

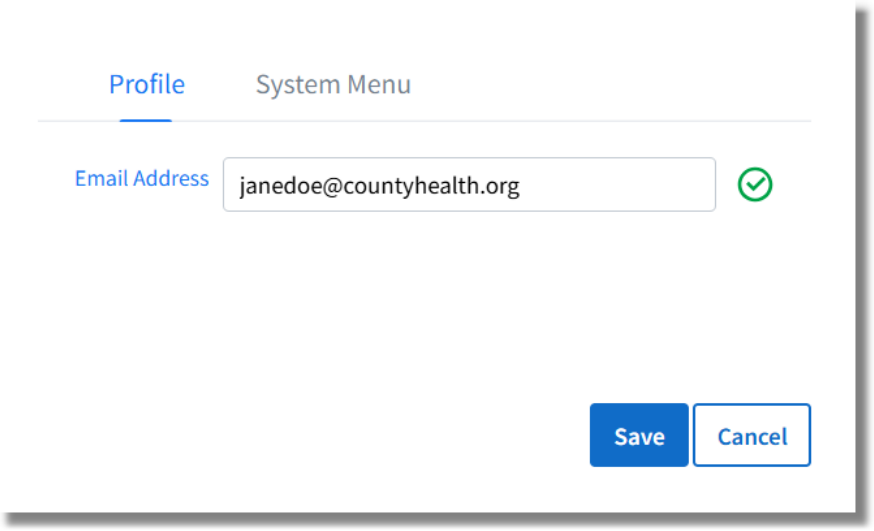
NOTE: *The label on this option will change depending on whether a verification link has already been sent.*

17.5 Changing E-Mail Addresses

If an email address has already been added to the user's login — whether it has been verified or not — it may be updated by either the user or the administrator.

User-Initiated: Changing an Email Address

Select **Web Client** > **User Profile** > **User Initials** > **Settings**

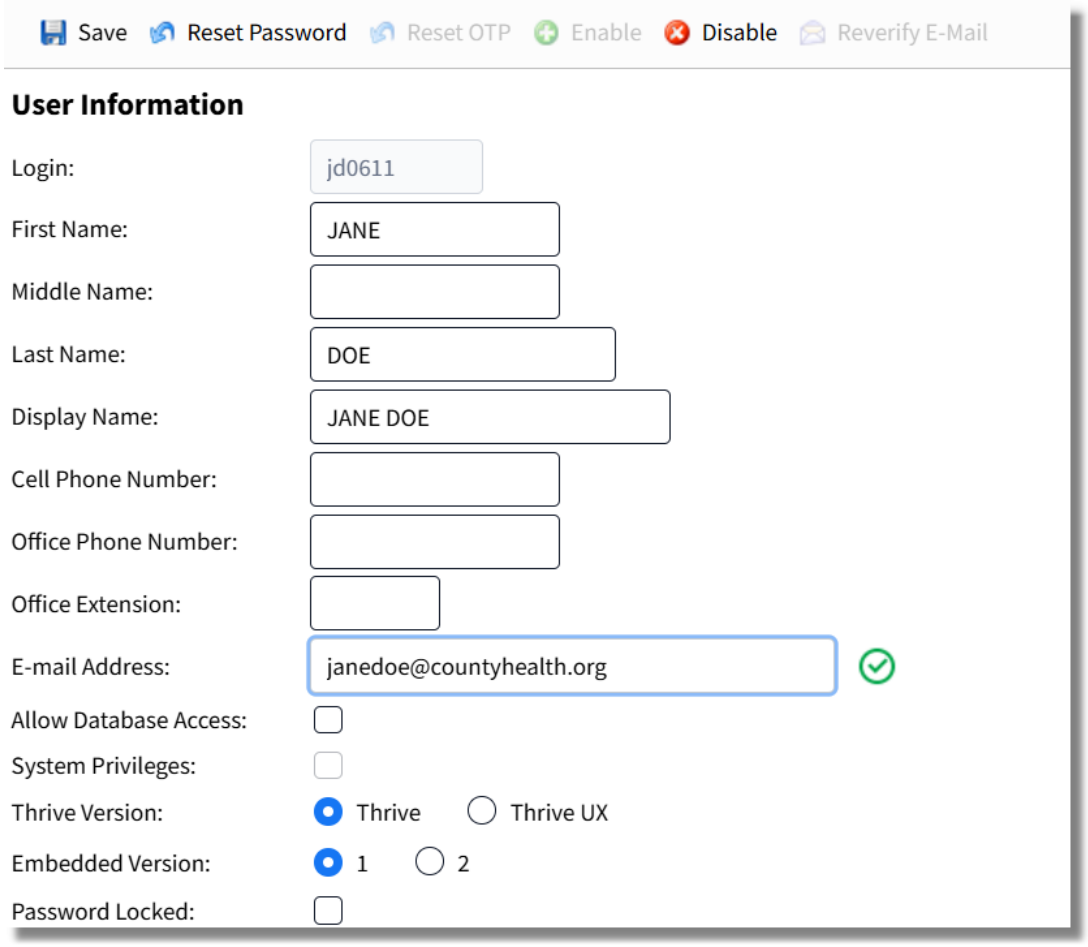


User Profile - Settings

- If an email address has already been stored on the user's login — either by a system administrator or by the user — it will display when the user accesses the Profile tab. The email address may be updated regardless of its verification status. The user may edit the email address and select **Save** to apply the change. A verification link will be sent to the new email address, and a notification will also be sent to the previous address.

Administrator-Initiated: Changing an Email Address

Select **Web Client** > **System Administration** > **Logins**



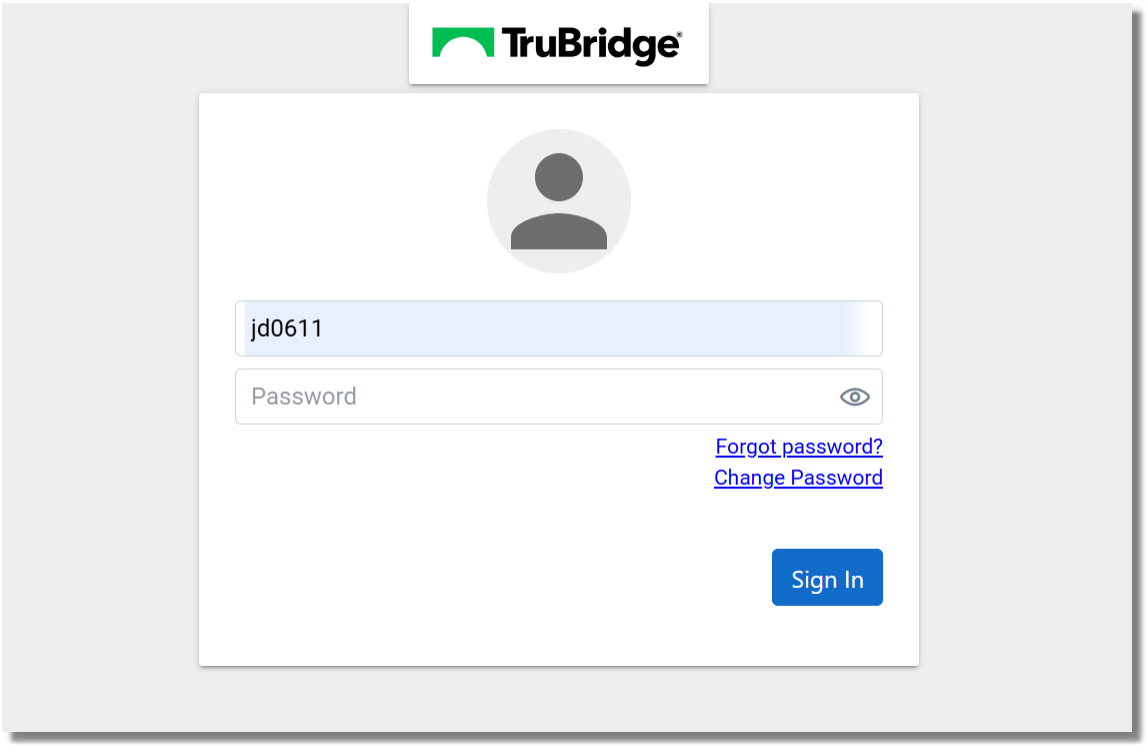
System Administration - User Information

- If an email address has already been stored on the user's login — either by a system administrator or by the user — it will display when the administrator accesses the User Information screen. The email address may be updated regardless of its verification status. The administrator may edit the email address and select **Save** to apply the change. A verification link will be sent to the new email address, and a notification will also be sent to the previous address.

17.6 Forgot Password Reset

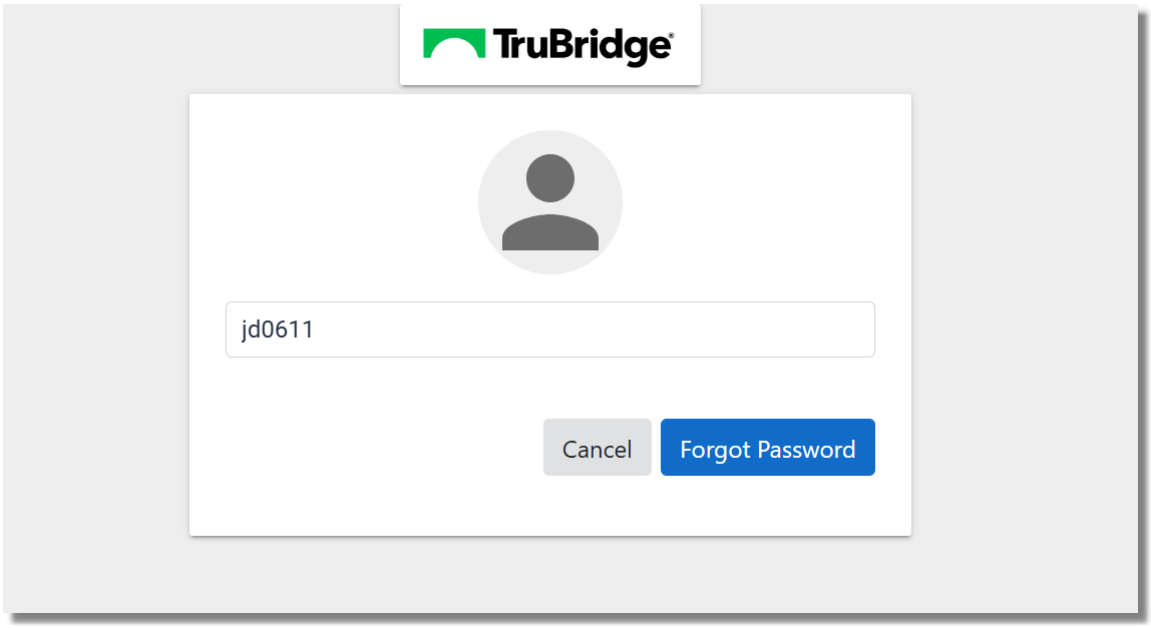
Once the user's email address has been verified, they may use the **Forgot Password** feature within Web Client.

Select **Web Client** > **Login Screen** > **Forgot Password?**



Web Client Login

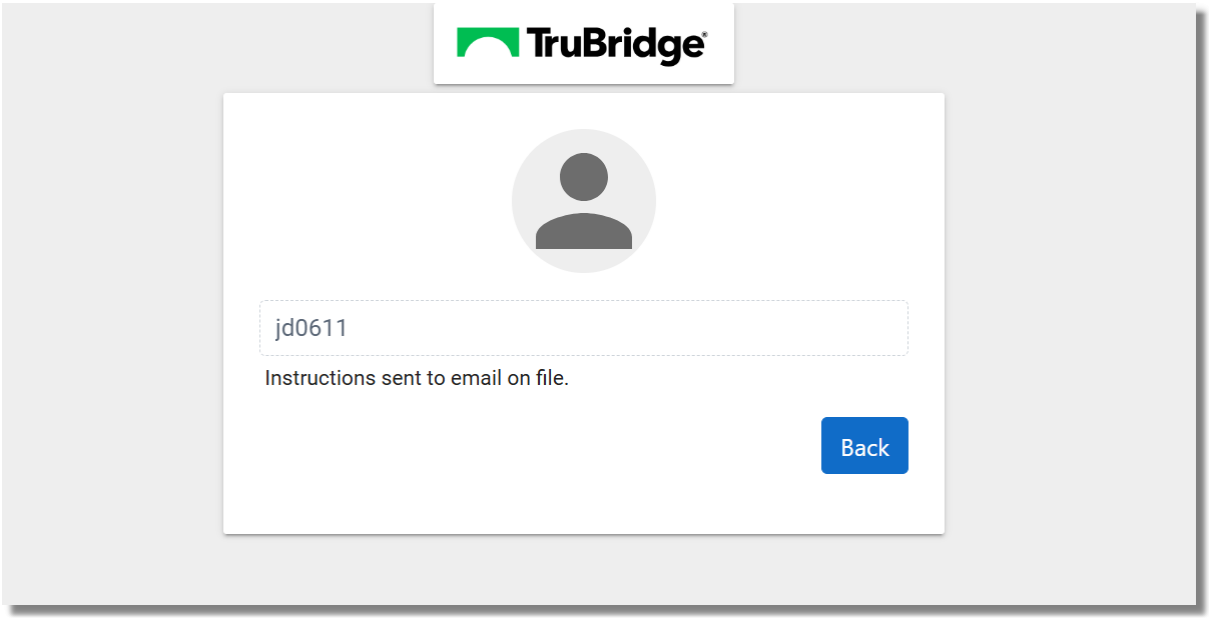
- On the Web Client login screen, the user should enter their user name and select **Forgot Password?**



Web Client Forgot Password

- If a verified email address is associated with the entered user name, the message **'Instructions sent to email on file.'** will be displayed. An email containing a **Reset Password** link will be sent to the user.

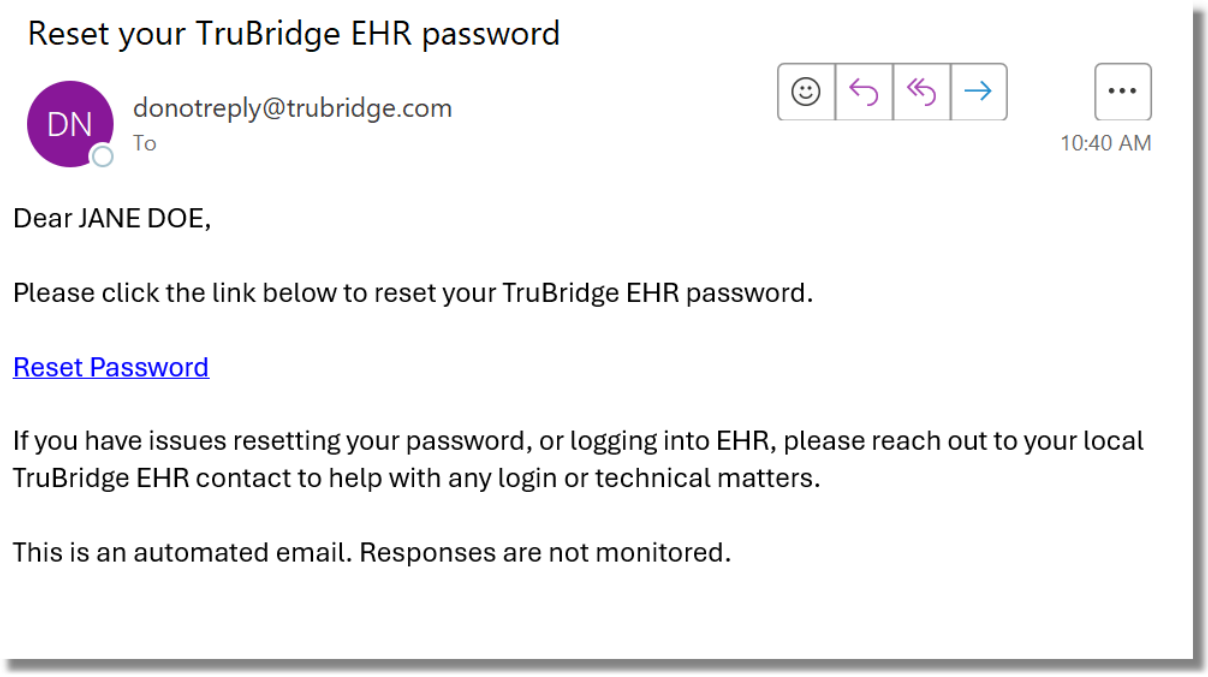
NOTE: *If no email address is associated with the entered user name, if the account is locked, or if the user name does not exist, a notification may be sent to the system administrators and to the user's email address (if available). These notifications require setup to be triggered. See* *Password Notification List* 149 *for more information.*



Web Client Forgot Password

- The user must select the **Reset Password** link to reset their password.

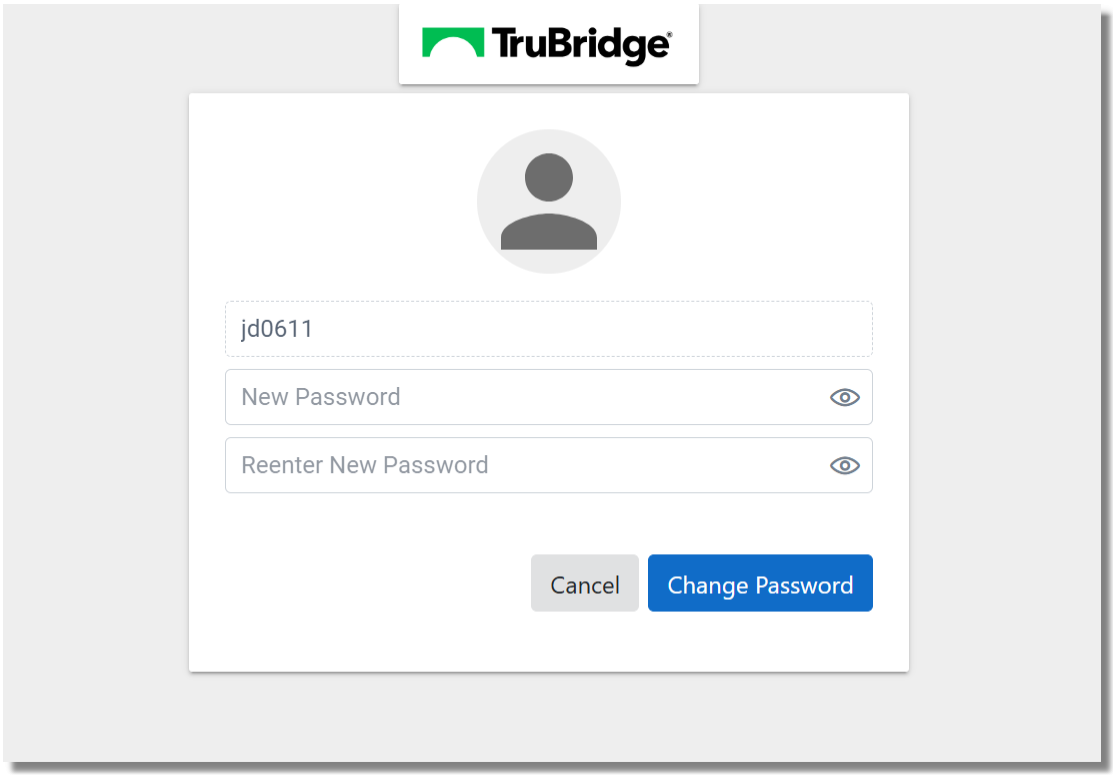
NOTE: *The reset password link expires after 60 minutes. If it is not used within that time, the user will need to select* ***Forgot Password?*** *from the Web Client login screen to restart the password reset process.*



Reset Password Email

- The user will enter their new password and select **Change Password**. The new password must comply with the facility's Password Policy, as outlined on the System screen. See Password Policy 98 for more information. Once the password has been successfully changed, the user may log in using the new password.

NOTE: *The "**A new password shall differ from previous password by ___ characters**" setting in the Password Policy is only enforced when a user changes their password. When a password is reset — either via System Administration or the Forgot Password feature — the original password is not available for comparison. As a result, this setting will not apply during a password reset, but all other Password Policy settings will still be enforced.*



Web Client Reset Password