Security Features

Reference guide

Last updated: January 10, 2025

Assurance Reimbursement Management™

Optum is a registered trademark of Optum, Inc. in the U.S. and other jurisdictions. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Optum reserves the right to change specifications without prior notice. Optum is an equal opportunity employer.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Table of contents

Introduction **3**
Account policy settings **3**
Default account policy settings 3
Password and account policy settings 4
The meaning of zero 4
Account policies 4
Checking account status - User master 5
How to modify account status 6
Access to data **6**
Determine your site security needs 6
Restrict user access **7**
Filter profile description 7
Setting up a filter profile 8
Setting filter profile restrictions 8
Report profile description 9
Setting up a report profile 9
To add a new profile: 10
To add or remove users in a profile 10
Notes 10
Field-level security **10**
Allowed IP addresses **11**
User profiles **11**
Auditing user activity **12**
Audit reports 12
Date-range filter 13
Password reset **14**
Troubleshooting **14**
User can’t log in 14
Account locked 14
Profile restriction violation 14
Support 14

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Introduction

Assurance Reimbursement Management™ (Assurance) provides robust authentication and access security controls. It also offers a selection of audit reports of user accounts and activities. The controls offer flexible implementation so that clients can customize the level of security necessary to meet their business needs. Measures that work for a larger business may be too burdensome and unnecessary for a smaller business. In contrast, measures that are reasonable for a smaller business may not be strong enough for a larger business.

Product access requires a valid username and password combination. This document explains the product security features, default values, and how to modify them.

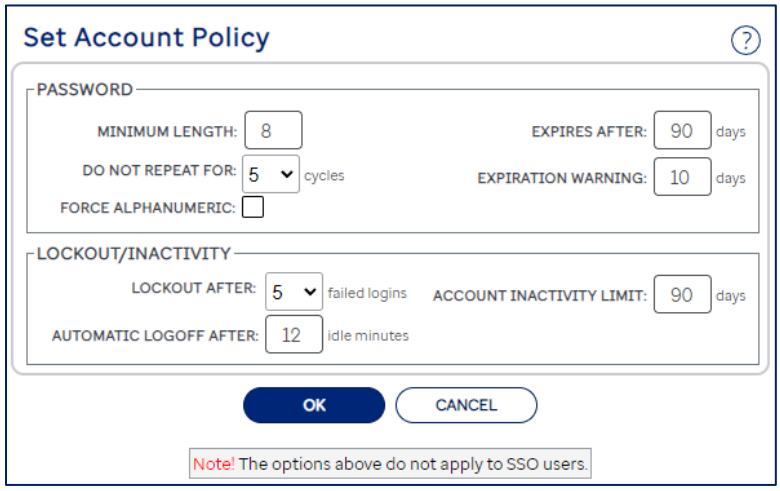
Account Policy settings allow specification of password requirements as well as automatic disabling, locking, or enabling of user accounts. (The account policies for Customer Identity Access Management (CIAM) are governed by CIAM, not set in Assurance.)

Restrict User Access allows limiting user to access to only specified claims. Claims that do not meet the named restriction criteria cannot be used or opened by the restricted users.

Account policy settings

Path: Maintenance, Security Setup, Set Account Policy

(default settings shown)



Default account policy settings

The default settings take effect for each client site when the client is created on the production system.

You can modify any of the settings in the table to suit your business needs. After making changes, click **OK** to save your work. Changes take effect immediately. Changes to password requirements will be enforced in **Change Password**.

To be able to change account policy settings, you must belong to a group that has group master rights to the **View Account Policy** and **Edit Account Policy** functions. To set these functions, follow this path: Maintenance > Master Setup > Group.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Setting	Default value	Description
Password		
Minimum Length	8	Minimum required length of a user password. You can set a higher value to enforce even longer passwords.
Expires After	90 days	Life cycle of a user password. Once the timeframe passes, the system forces users to change their passwords. The longest duration allowed is 90 days. You may set a lower value to force users to change passwords more frequently.
Do Not Repeat for [ ] Cycles	5	How often a user can reuse a password. A “cycle” is defined each time the user changes the password.
Expiration Warning	10 days	Timeframe when the system should remind a user to change the password before it expires.
Force Alphanumeric	Unchecked	If checked, requires the user to include at least one number in the password.
Lockout		
After [ ] Failed Logins	5	How many successive times a user can fail to log in before the system will lock out the account.
Account Inactivity Limit	90 days	Based on the last logon date, how long an account can remain inactive before the system disables it.
Automatic Logoff After	90 idle minutes	How long a user session may stay open without activity before the system logs off the session.

Password and account policy settings

This date starts the clock for the password expiration, repeat cycle, and account inactivity timeframes.

There are two mandatory requirements for all user passwords. You cannot change these requirements:

1. **Uppercase and lowercase**: Every user password must include both uppercase and lowercase letters.
2. **Special characters**: Every user password must include at least one of these symbols:
   ~ ! @ # $ % ^ & * ( ) _ + - = | < > ’

The meaning of zero

A zero (0) in the following fields on *Set Account Policy* means the timeframe is not defined:

- **Account Inactivity Limit:** If zero is entered, security will never disable accounts due to a lack of activity.
- **Automatic Logoff After:** If zero is entered, security will never logoff a session due to idle time.

Account policies

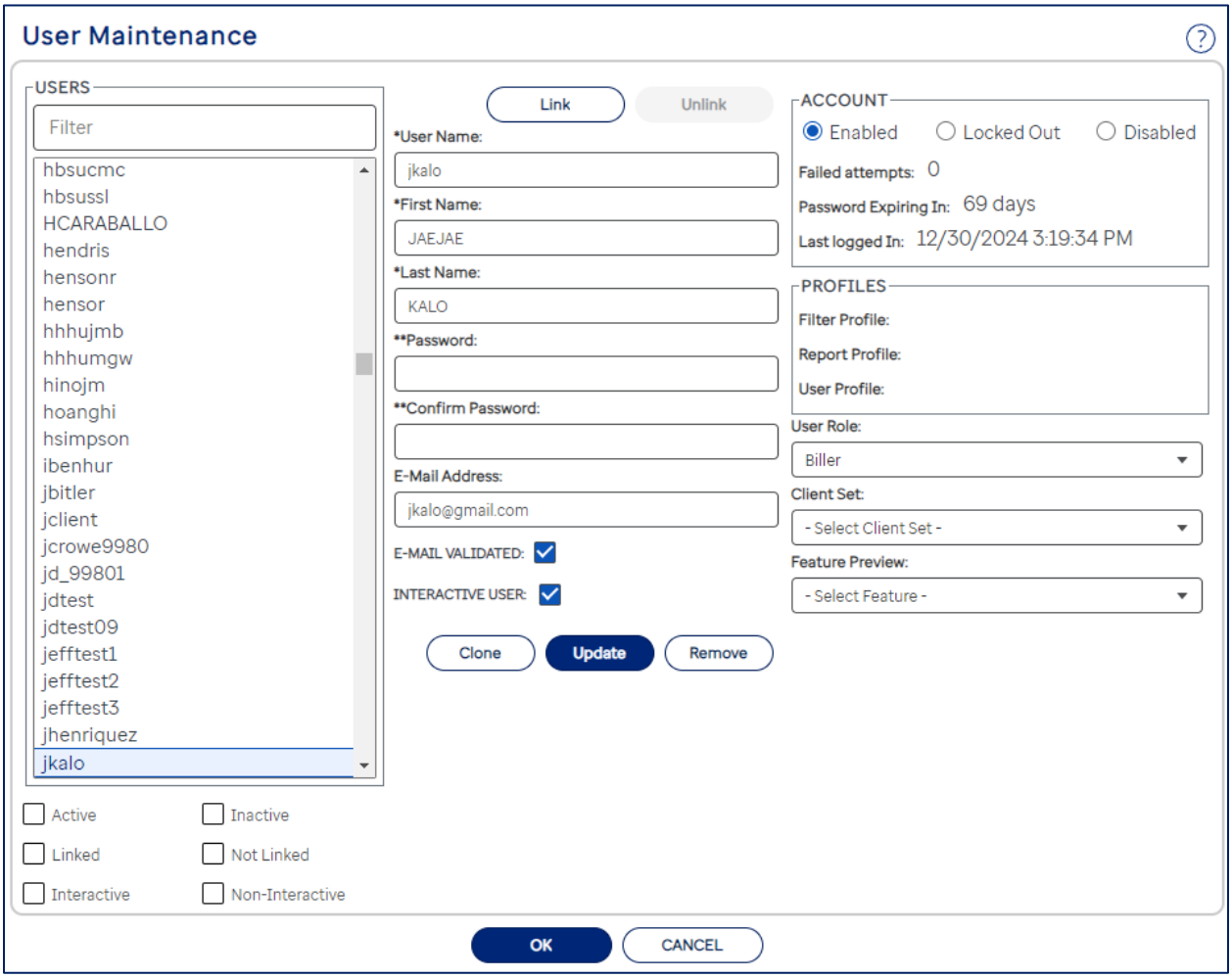
Once users are set up with a One Healthcare ID (OHID) account, the OHID account policies apply when they log into Assurance. Settings for password resets, lockouts, failed login attempts, etc. are managed by OHID. A warning will be displayed before a session expires, allowing users to extend the session.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Checking account status - User master

To determine if any account is enabled, locked out, or disabled, open the **User Maintenance** page (Maintenance > Master Setup > User). Check the **Account** information: enabled, locked out or disabled.

Note: To review user information, you must belong to a group that has rights to *View Users*. (Group Master).



Entry	Description
Failed attempts	Number of consecutive failed log in attempts for the user. This value is reset to ‘0’ upon a successful login.
Password expiring in	Total number of days remaining before the current password will expire.
Last logged in	System date and time of the user's last successful log in.
Filter profile	Name of the assigned filter access profile. This item is empty if no profile is assigned. Refer to the Restrict User Access section for more information.
Report profile	Name of the assigned report access profile. This item is empty if no profile is assigned.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

	Refer to the Restrict User Access section for more information.
User profile	Names the assigned User Profile or displays **Multiple User Profiles Configured** when the user is a member of more than one profile set up on the **Maintenance** menu, **Master Setup**, **User Profile** feature.

- If the account is enabled, the user can log on and has access to the functions defined for the user in **Group Maintenance**.
- If the account is locked out, a user cannot log in. A locked account may be enabled manually by the site administrator or automatically by the system. The system locks out an account when the user has exceeded the threshold of allowed consecutive failed login attempts. Lockout options are set in **Set Account Policy**.
- If the account is disabled, a user cannot log in. A disabled account must be manually enabled by the site administrator. Unlike locked accounts, there is no way to automate enabling. The site administrator may disable an account as needed according to the site's security procedures, or the system may automatically disable an account due to inactivity.
- Viewing and making changes in user maintenance requires that the user be in a group that has rights to View Users and Edit Users. (Maintenance > Master Setup > Group)

How to modify account status

1. Open **User Maintenance**: Maintenance > Master Setup > Group
2. Modify each user account as desired.
3. Click **Update** after completing changes to each user account.
4. When all changes have been made, click **OK**.

Access to data

General access to features is controlled by placing users in groups that have rights to specific functions (e.g., View Claims). These group security functions control users' ability to navigate and access system features.

Restrict user access (described below) is an optional feature for higher security if your site's security policy requires tighter control over users' access to personal health information (PHI).

Determine your site security needs

Before setting up any access profiles, carefully consider your security needs. You may not need to use the **Restrict User Access** feature. If you do want to use it, determining what you need before the setup will help make the implementation process more efficient.

1. What is your security policy and practice? Do you need to control access to product functions, claim data or both?
   - To control feature access, use the group functions in Group Maintenance.
   - To control data access, set up security profiles in Restrict User Access.
   - There is also a User Profile that controls data access within these newer features: Claim Assignments based on the newer Payer Status Rules and the enhanced Reconciliation Manager Dashboard.
2. If data access restrictions are needed, what kind of profiles do you need? How many?
   - Do you need to restrict users to viewing and working with only certain types of claims?

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

- Do you need to restrict users to creating certain reports?
- You may need several different profiles to fit various jobs like billers, supervisors, management, site administrators or other work functions.
- Each user may have one filter profile and one report profile at any given time.

3. Which options need to be restricted within the profile?
   - Profiles should be based on workflow. For example, if billers work claims and remits according to the line of business and patient last name, then build Filter Profiles based on the LOB and Patient Last Name criteria.
   - Remember to accommodate employee substitutes during office absences. If billers back each other up, their security profiles will need to include the appropriate restrictions.
4. There is a more granular security level: **field-level security**. Field-level security allows you to set specified claim fields as view-only for specific users at your site. When these users are in a claim, they can view the contents of the secured field, but they cannot make changes to it. If you need this level of security, contact Assurance support to learn more about it.

Restrict user access

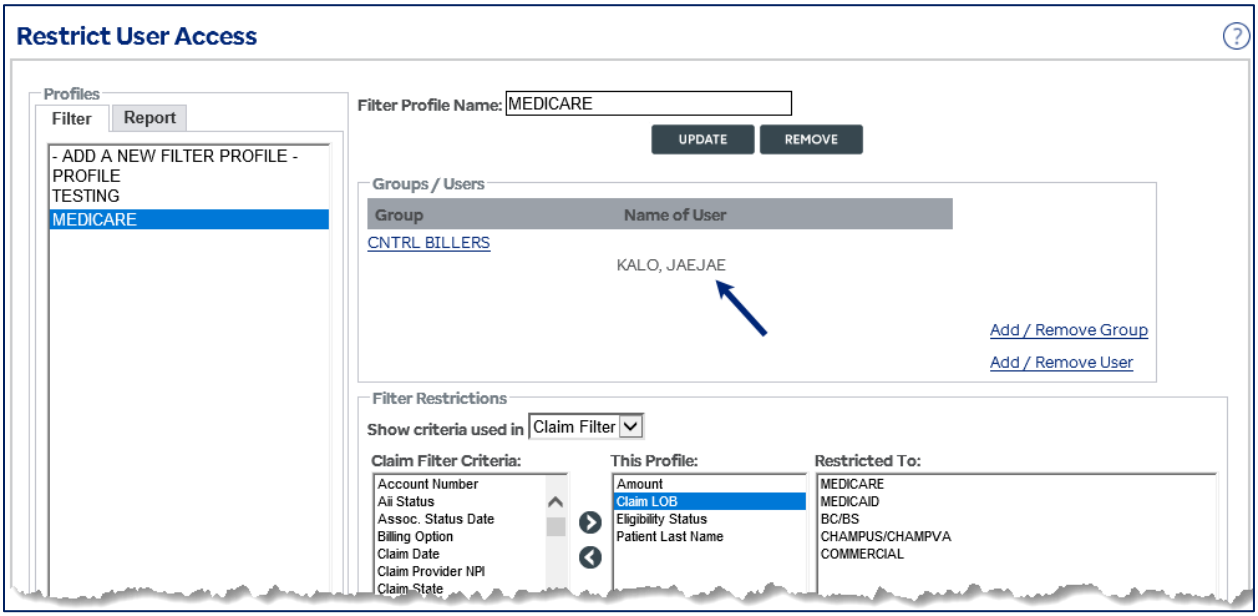
Path: Maintenance > Security Setup > Restrict User Access

You can restrict the view and modification of data based on users' business roles. For example, a user may be restricted to viewing and modifying Medicare claims for a specific facility. Use *Restrict User Access* to set up this restriction.

Many users may be assigned to the same profile, but an individual user cannot belong to more than one filter profile or more than one report profile.

Filter profile description

Restrictions set up on this page are positive restrictions. For instance, the illustrated profile will display only claims for patients that have last names to any user in the *Cntrl Billers* group and to *Jaejae Kalo*. When these users set up a claim filter to get claims for any purpose, before the claims are used, all claims that do not meet these restrictions are removed from the working group. (A message also displays to tell them that claims were removed from the working group based on their restriction profile.)



© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Setting up a filter profile

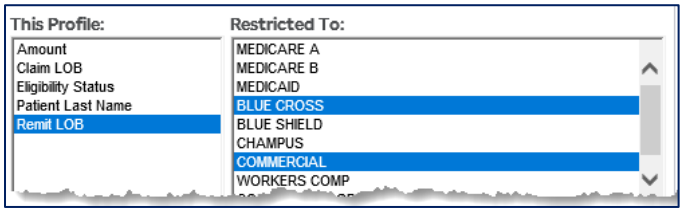
1. Enter a **name** for the restriction and click **Add**.
2. In Groups/Users, use either or both options to open a list of groups or users and select the ones that should be restricted by this profile.
3. In the Filter Restrictions segment, select the filter type with which you want to apply restrictions (claim, filter, or both). The list of restriction criteria will change to display only the criteria that belong to the filter you have chosen.
4. From the Filter Criteria list, select an item and move it to This Profile.
5. To set the restrictions for the new item, select or type in the Restricted to: area. Any list in Restricted To is a multiple-select list.
6. Repeat steps 4 and 5 for each filter criteria you need to set.
7. Click **OK**.

Setting filter profile restrictions

For a selected criteria item, the “Restricted To” area will display a list of options, an empty field for user input, or calendar controls for date fields as appropriate. This section illustrates an example of each kind of criteria item.

List of options

Some criteria items are associated with a list of options. These items include but are not limited to the line of business, payers, and facilities. The “Restricted To” area will display the available list of options. One or more limitations may be selected.



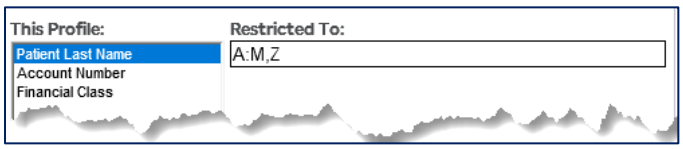
In this illustration, the profile limits the user to viewing Blue Cross and Commercial remit data. (There are also restrictions for the Claim LOB and the Patient Last Name.)

- To select multiple adjacent items, click the first item and drag the pointer until all desired options are selected.
- To select multiple items that are not adjacent, click an item. Press and hold the CTRL key, then click each additional item you want to select.

Note: There are separate lists for claim LOBs and remit LOBs. If you only restrict the claim LOB to Medicare in a profile, a user who has functional access to remit data can still view claims for other lines of business through the remit filter. Both claim LOB and remit LOB items need to be restricted to Medicare.

Empty field for user input

Some criteria items are associated with a field for user input. These include but are not limited to patient last name, account number, and financial class. The user may enter one value or a range of values.



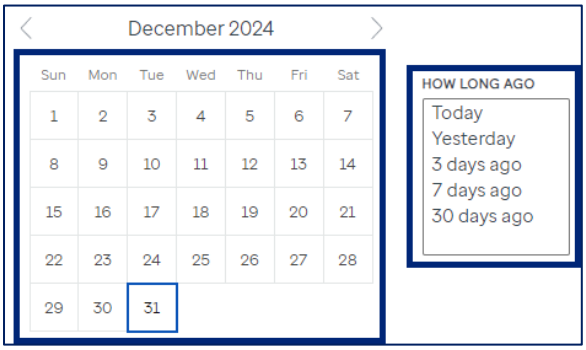
© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

In this illustration, the profile limits the user to viewing and modifying claims where the patient last name begins with a letter from A through M or with the letter Z.

- Use a colon [:] between two values to indicate a range such as A through M.
- Use a comma to separate items within the entry.

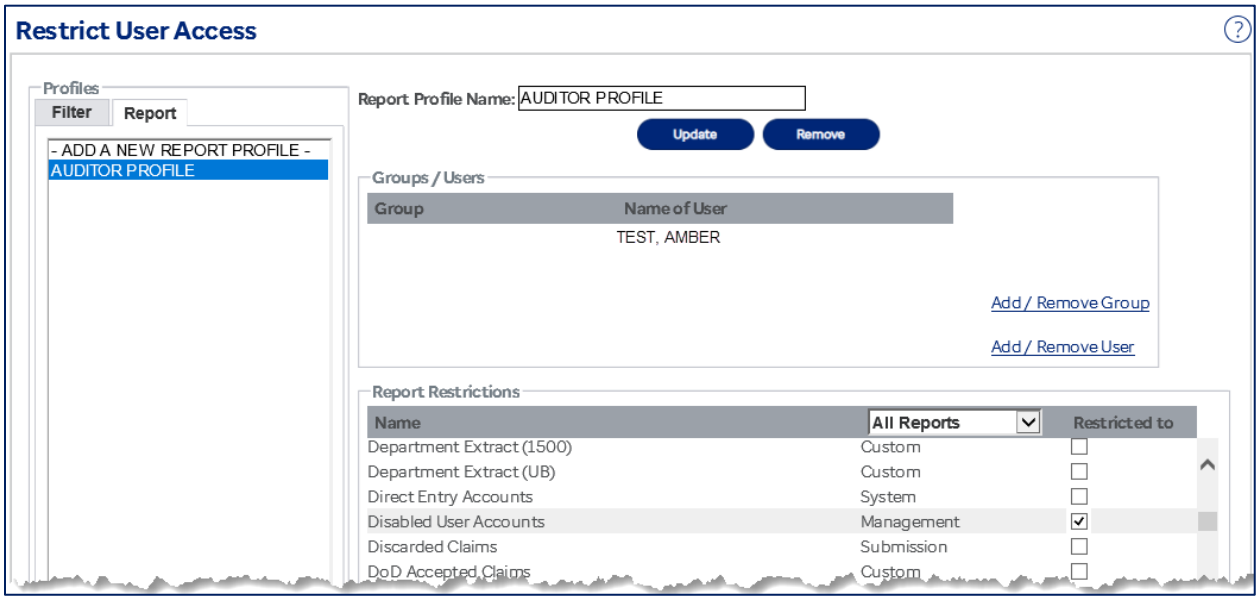
Date fields

Some criteria items require a date. These items include but are not limited to the Date Released or Discharge Date. For these items, the *Restricted To* area will display a calendar control for easy date selection. Choose a specific date from the calendar panel on the left or choose a relative date from the "How long ago" panel on the right.



Report profile description

Access to reports is controlled through a Report Profile by selecting the individual reports a user is limited to viewing and creating. A user may only have one Report Profile. In this illustration, the *Auditor Profile* is assigned to AMBER TEST. This report profile restricts AMBER TEST to creating and viewing certain management reports such as Disabled User Accounts.



Setting up a report profile

You must belong to a group that has rights to both *View Restrict User Access* and *Edit Restrict User Access* functions in *Group Maintenance*.

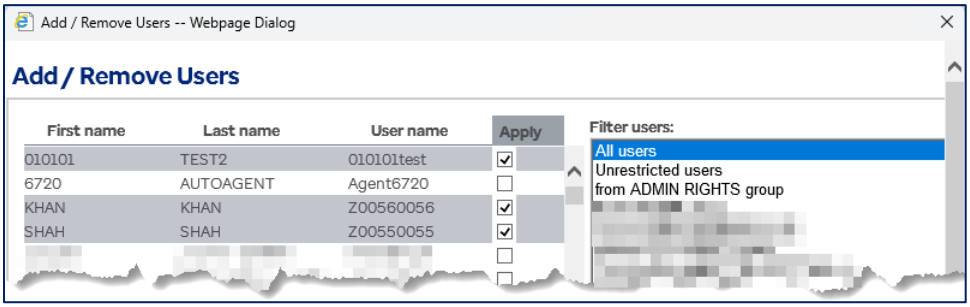
© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

To add a new profile:

1. Open Restrict User Access: Maintenance, Security Setup, Restrict User Access.
2. Click the Report tab at the top of the Profiles list.
3. Enter the profile name and click the **Add** button.
4. In Groups/Users, use either or both options to open a list of groups or users and select the ones that should be restricted by this profile.
5. In Report Restrictions, check each report you want this profile to be able to create. (The Reports list can be sorted by Report Type.)
6. Repeat steps 3-5 for each additional report profile.
7. Click **OK** after adding the desired new profiles to save your work.

To add or remove users in a profile

1. Click one of the *Add/Remove* links in the Groups/Users area to open the *Add/Remove Users* window.
2. Check each user that should be added to the profile. (**Tip:** To quickly assign an entire Group, use the Add/Remove Groups link.)



3. Click ***OK***.

Notes

- When setting up profiles, if the user already has another profile of the same type, a message will display to confirm that you want to change the assigned profile for the user.
- To see the profiles to which a user is attached, open **User Maintenance** and click the user's logon name. If the user is restricted by a profile, the name of the profile will display in the **Account Status** section.

Field-level security

Path: Maintenance > Security Setup > Field Level Security

Field-level security controls the rights to make changes to claim fields. The rights are attached to the groups set up in Group Master. Each user in the group has the same field-change rights. When members of the group view claims, all fields are visible, but the users cannot change the fields that have been designated as read-only for their group.

Field-level security works like other product security: The default is no 'restrictions' and the security pages are used to restrict those wide-open rights according to user name or group. Unless you specifically restrict rights, all fields are open to all users.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Before you can set up Field-Level Security, your groups must be set up in the Group Master. Once the groups are created, follow these steps to make fields read-only:

1. Select the group name from the **Groups** panel.
2. Select the fields you want to restrict for the group from the **All Fields** list.
3. Click the arrow button to move the list to **Read-Only for this Group**.
4. When all restrictions are in place for the desired groups, click **OK** to save your settings.

Allowed IP addresses

Path: Maintenance > Security Setup > Allowed IP Addresses

Each computer in your network has a unique IP address that consists of a network ID plus a computer (node) ID. Use this page to name the IP addresses (local or remote) that are allowed to access this product. If the **Address** list is empty, all of your currently allowed IP addresses can connect. This is the default setting.

If your business policies require blocking or limiting access to this product, you can specify the IP addresses from which the product will accept a log on. Allowed IP Address makes connection to the product an invitation-only activity. You add the IP addresses of each computer that should be able to access the product. When Allowed IP Addresses is used, this product will accept a log on from only the computers on your **Allowed Addresses** list.

You can add new addresses, remove existing addresses, and change existing addresses.

Follow these steps to add an address to the Allowed Addresses list:

1. Type the address into IP Address.
2. Click Add. You can add multiple addresses by typing an address and clicking Add between addresses or by using a wild card as shown in the Notes below.
3. When you have added all the addresses you need, click OK to save your work.

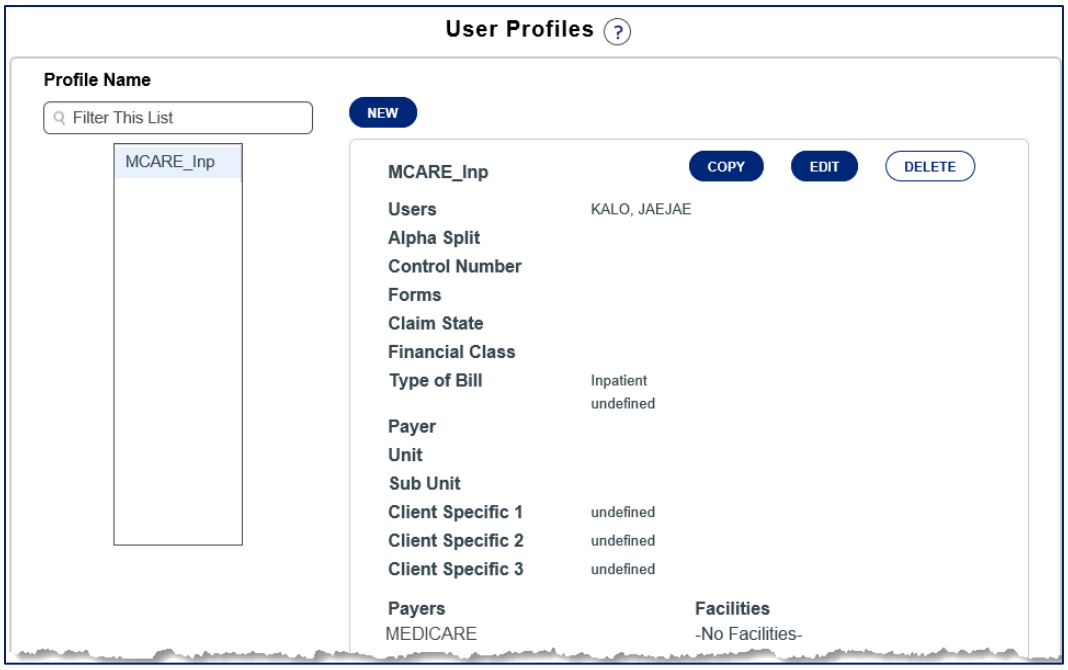
User profiles

Path: Maintenance > Master Setup > User Profile

The user profiles master allows you to associate your users with specific claims based on claim criteria, payers, and facilities. This association is useful with claim assignments based on the Payer Status Rules (new) or with using the Reconciliation Manager Dashboard. You need the User Profiles to define which user has the responsibility for the claim assignment or for reviewing the claim status. In the sample user

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

profile below, Jaejae Kalo can only access inpatient claims for Medicare payers through the two features controlled by User Profiles.



Follow these steps to create a new user profile:

1. Click the **New** button.
2. Type a **Profile Name**. (limited to 25 characters)
3. Choose the profile members. (**Users Available** and **Users Selected**)
4. The system displays enabled users from your site's User master.
5. Choose the associated payers. (**Payers Available** and **Payers Selected**)
   – You can leave this item empty to instruct the system to include all payers.
6. Choose the associated facilities. (**Facilities Available** and **Facilities Selected**)
   – You can leave this item empty to instruct the system to include all facilities.
7. Select targeted claim criteria as needed.
8. Click the **Save Profile** button. The system adds the item to the **Profile Name** list.

Auditing user activity

There are several useful reports to audit system and user activity. These reports are described briefly in this section. The entry in parenthesis after each report name is the Type in ***Create Reports***. In addition, Help includes a sample of each report: Open *Help*, *Help Index* and drop down to *Sample Reports* at the end of the index.

Audit reports

The following reports provide managers with visibility to audit functionality in Assurance:

- Claim Changes Summary and History (Unreleased, Released): For the selected fields, the Summary report lists the original and current data in selected fields, and the History report lists all changes to the selected fields. Each change includes the ID of the user or product function that made the change and the date it was made.
- User Master (System): This report is a record of all user accounts.

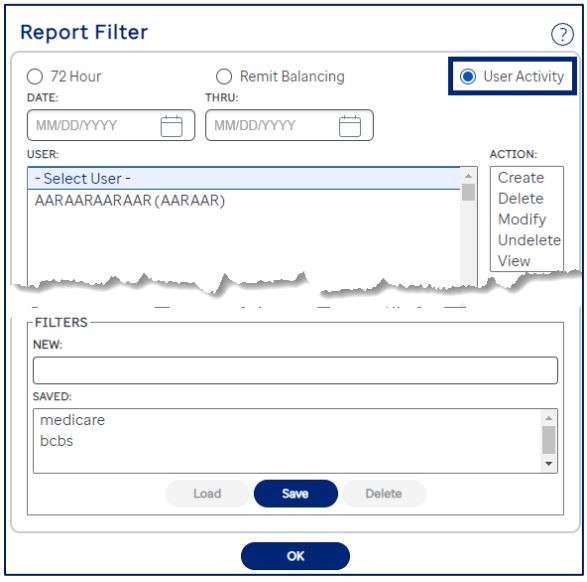
© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

- Group Master (System): The functions assigned to each group are listed in this report. The functions determine which user or users can navigate to and access a product feature such as “View Remits”. (A group may be comprised of one user or many users.)
- User Master (System): Lists information about site users with a log in account. Includes the name, group assignment, account status, and the assigned user profile.
- User Profile (System): Shows the information for each user profile set-up which allows you to associate users with specific claims based on claim criteria, payers, and facilities.
- Web Site Logging (Miscellaneous): Check this report for the user name, login date/time, logout date/time, and the session duration for any selected user and time frame.
- Failed Login (Miscellaneous): This report lists the user name, attempted login date and time, and system error remarks for any selected user and time frame.
- Disabled User Accounts (Management): The report displays the user name (login) for disabled accounts as well as the date and time that the account was disabled.
- Last Access By User (Management): This report is a record of the last access date for each site user. The report includes the user name (login), and the last access date.
- User Activity Exceptions (Management): Provides a record of users who attempted to access information outside their security profile restrictions. (See the **Restrict User Access** section in this document for information about security profiles.)
- User Activity Audit Reports (Management): There are three user activity audit reports: Claim, Remit, and Report. When a user selects one of these reports to create, a Report Filter window is activated to allow selection of a time frame, user list, and action type for the report. The finished report provides a record of user activity related to claims, remits, or reports.

Date-range filter

Path: Reports > Report Setup > Date-Range Filter

The User Activity reports use the Date-Range filter. When running a report manually, just set the filter to get the data you need. Before setting up automation for these reports, open the Date-Range Filter and set up and save the filters you will need



- If a specific user or list of users is not selected, the reports will include all users, ***even Product Support associates who viewed data to troubleshoot an issue for you.*** Both Product Support user names and product function names are prefixed with ***ndc*** for easy identification.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

  - There are five user actions that are tracked and reported: View, Modify, Create, Delete, or Undelete.
  - If a user prints claims, the system will record and report a *view* action for the selected claims for that user. It is not recorded as a *print* action because the actual printing is handled outside on the local system through a third-party product such as Adobe Acrobat.
- Time span of these reports is limited to between one and thirty-one (31) days.

Password reset

Password reset will be done from the OHID login screen .

Troubleshooting

User can’t log in

If a user is unable to log in, they can confirm that they are using the correct email address for OHID.

- You may have a different email address on file for Assurance than what was used to create your OHID account. Contact support for assistance.

Account locked

Click **Continue** on the Account Locked page. When the Account Locked: Verify Your Identity page opens, use the verification method you set up when you created your OHID account.

Profile restriction violation

When users request claims outside of their profiles, a message tells them why certain requested claims are not in the working group. In addition, an entry is written to the Security log that details the username and the action that violated the restrictions. Users may need to check with the local site administrator to verify their assigned profile restrictions.

For example: A user is restricted to claims that contain a Financial Class code of SNF.

If the user filters for claims that contain Financial Class XYZ, all claims in that group will be off-limits and a popup message will display on top of the filter: *“The filter requested claims restricted by your security profile. Element name: “Financial Class”.*

If the user filters for unreleased claims, some claims will be allowed and some will be off-limits. When Refine is clicked, the restriction warning displays at the bottom of the page. The claims in the selection list are the allowed claims; the off-limits claims are not displayed for selection.

If the filter’s Continue button is clicked, no message displays, the first allowed claim is opened, and the claim list contains only allowed claims.

These violations will be included in User Activity Exception report.

Support

For additional issues, refer to the One Healthcare ID toolkit.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.