System (All Modules)

Release Notes December 2024

The document details recent updates to the **ADMINS Unified Community (AUC) for Windows SYSTEM** module aimed at enhancing user experience and security.

- **Rebuilding Security Button**: A new button has been added to streamline the process of rebuilding account security, making it easier to choose the right option and improve efficiency.
- **Suspending Inactive Users**: An automated process now suspends inactive accounts weekly, with email notifications sent to users two weeks prior to suspension.
- **Tracking User Logins**: Detailed logging of user login attempts, including failed attempts and password changes, has been implemented to enhance security.
- **Automated Password Expiration**: New features enforce regular password updates and prevent the reuse of recent passwords, enhancing account security.
- **Enhanced Logging of Login Activity**: Additional details about login activity, including client computer names and failed login attempts, are now logged to provide more information about user activities.

CONTENTS

1 Rebuilding Security Button [Enhancement]

Users sometimes report that the rebuild for account security after making a change is taking a long time. This often occurs because the user has selected to rebuild all security for all years instead of just the security for a single user for the current year.

To make it easier to choose the right option, **ADMINS** added a button directly on the screen that will rebuild the security in the quickest way. To use this feature from the menu, select:

Ledgers ▶ Account Maintenance ▶ Account Security

The "old" method under the Actions button is still available when needed.

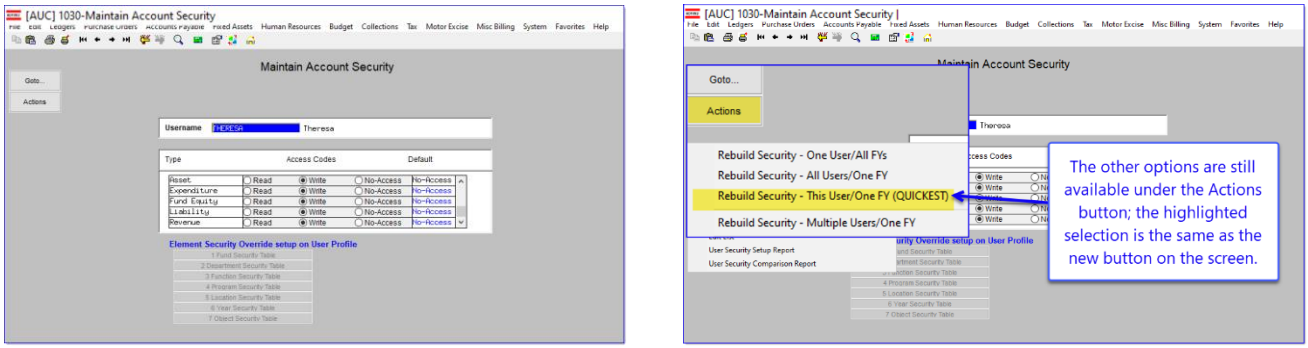
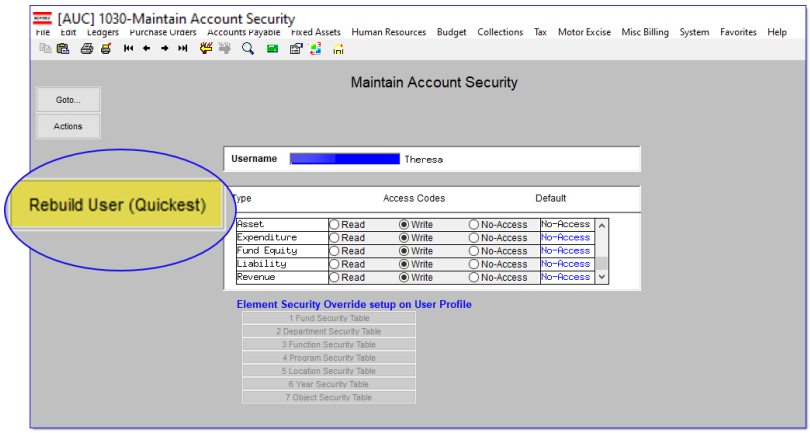
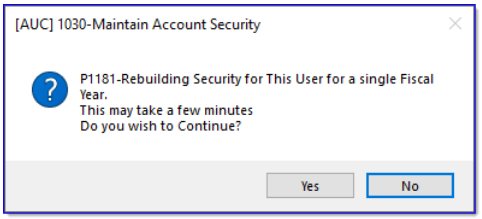


Figure 1 Before – the user had to click on Actions and select from the drop-down list

Most of the time the new button on the screen is the one to use.



Click Yes on this prompt to continue.



Notice that the rebuild is for this user for a single Fiscal Year. Enter the Fiscal Year here:

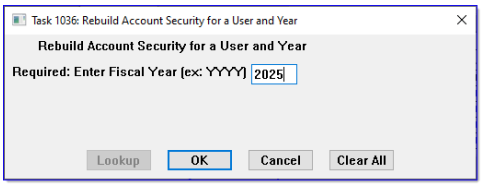
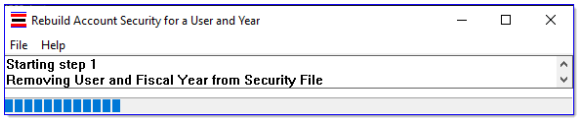


Figure 2 After – ADMINS added the Rebuild User (Quickest) **button directly on the screen**

The progress bar will appear, and upon completion, return you to the Maintain Account Security screen. To view the accounts for which the user has access, follow the directions here in Section 3.



[ADM-AUC-GL-8565]

2 Suspending Inactive Users [Enhancement]

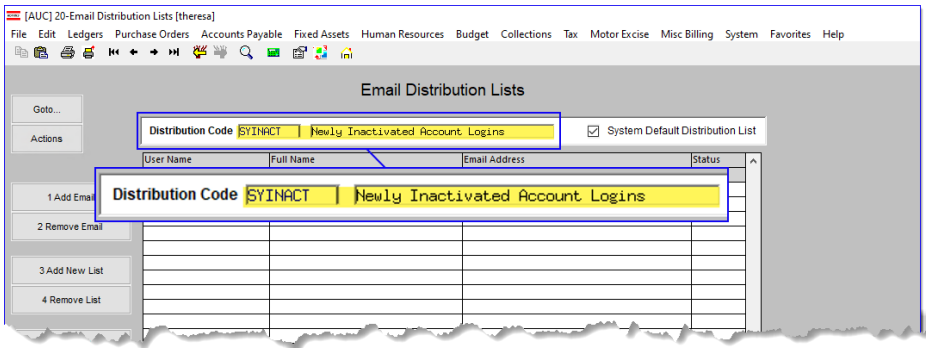
ADMINS added a distribution list and a new feature that sends an e-mail two weeks prior to notify users of their inactivity and the intent to suspend their accounts on the AUC system. This enhances the feature announced in the June 2024 release notes that allows the automatic suspension of inactive accounts.

2.1 Weekly Email of Suspended Accounts to SYINACT Distribution List

Inactive accounts are suspended weekly by an automated process. Module Control #65 specifies the inactivity duration that leads to suspension.

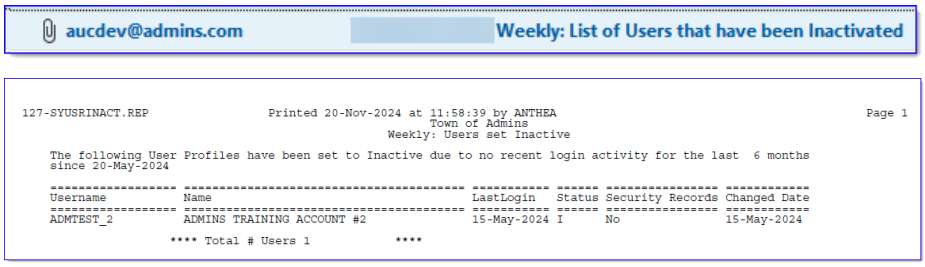
The list of newly inactivated users will be emailed each week to the SYINACT distribution list.

Superusers can add supervisory staff usernames to the list as needed. See SY-150 Email Distribution Lists for instructions.



The report will show the Username, the name of the user, and their last login.

The report will be emailed as an attachment and will look like this:



When an annual task nears, the superuser can re-activate suspended users and prompt them to log in, allowing proactive account management.

If no users are inactivated, the report will not be generated.

[ADM-AUC-SY-8356]

2.2 Email Notice to Users of Intent to Suspend an Account

Users are inactivated if they have not logged in before their expiration date.

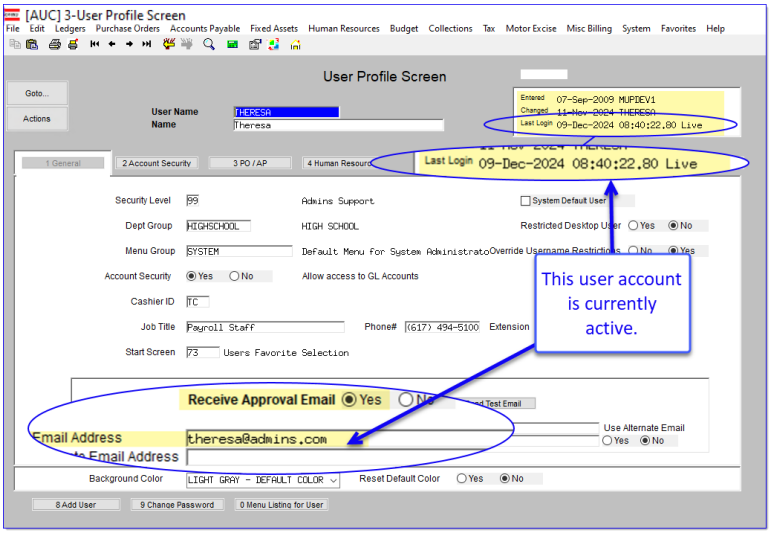
For instance, on sites with a six month expiration window, users who haven't logged in since 20-May-2024 would be “suspended” or “marked inactive” on 20-November-2024.

The notification period is 14 days from the suspension date, in this example, from 05-November-2024 through 20-November-2024.

Up to two reminder emails are sent: the first ~14 days before account expiration, and the second ~5 days before. If users do not log in when reminded, their accounts will be deactivated.

Two emails are sent to allow for users on vacation, etc., to have time to respond.

The notification is sent if there is an email address present on the User Profile screen:



The emails include expiration dates, steps to prevent suspension, and instructions for requesting reactivation after suspension.

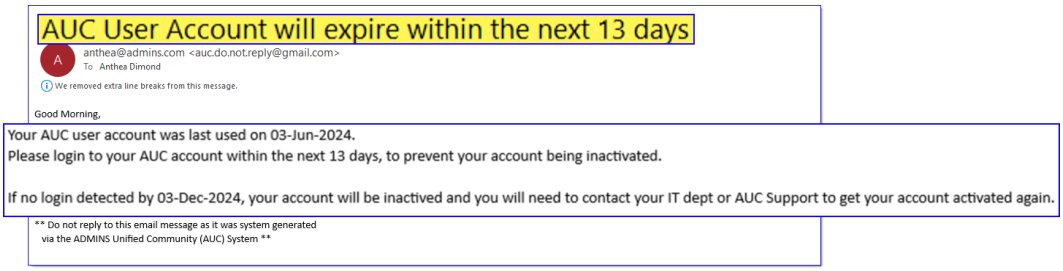


Figure 3 Email example sent two weeks before the username expiration date

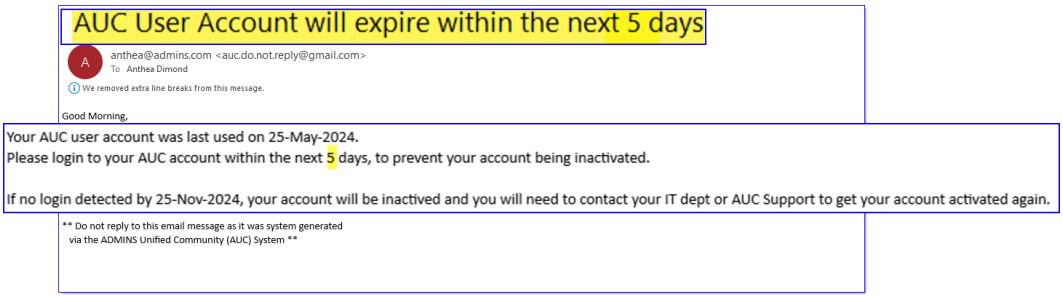
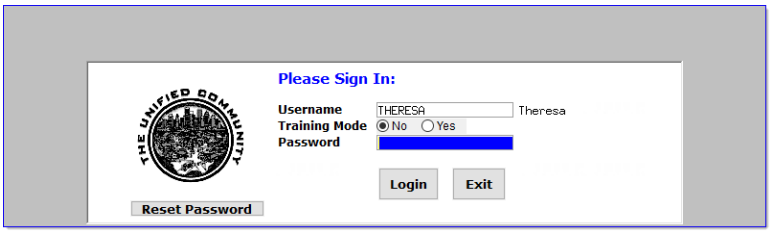


Figure 4 Email example sent the following week

[ADM-AUC-SY-8356]

3 Automated Password Expiration

ADMINS incorporated two new features regarding user passwords. Note that these are AUC application passwords, not Microsoft server domain passwords.

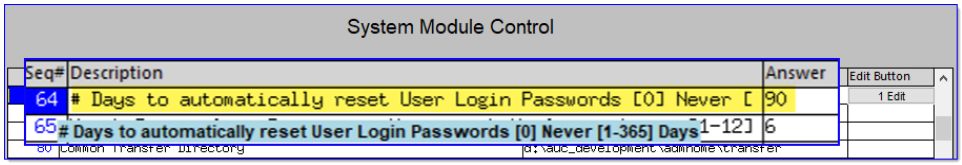


Password Expiration: A new Module Control 64 has been added, which checks the last password change date. If the number of days since the last change exceeds the value set in Module Control 64, users will be prompted to change their password. This feature ensures that passwords are regularly updated to enhance security.

Check for Re-used Passwords: When a user changes their password, the system checks if the new password matches any of the last three passwords used. This prevents users from reusing recent passwords, further enhancing security.

These features are designed to improve the security of user accounts by enforcing regular password updates and preventing the reuse of recent passwords.

3.1 Automated Password Expiration After # Days



ADMINS added a new Module Control 64 (note: during the December 2024 software updates, this will be set to 0 at all sites).

If MODCTR 64 is greater than zero, it checks the last password change. If it exceeds the number of days set in MODCTR, a message will display. The number of days (e.g., 90) can vary by site.

If they are forced to change their password it will log that in the log history screen.

Last Date	Last Time	Login Type
21-Oct-2024	16:10:00.86	Required Password change due to reset timeout reached

3.2 Check for Re-used Passwords

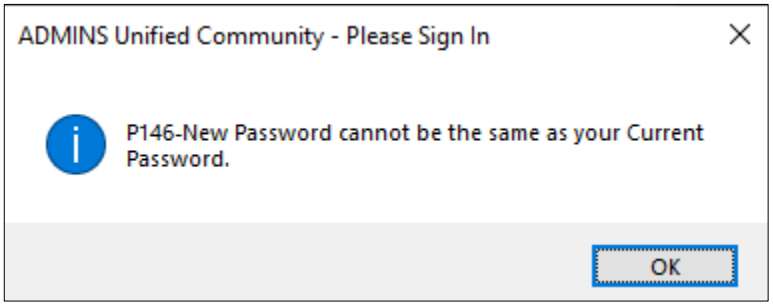
If a user changes their password for any reason, the system will check to see if the new password has been used among the last three passwords they set (this is independent of the first change). Even if the site does not enforce a password change, it will still ensure that the new password is not the same as any of the last three passwords used.

When a user enters a new password and clicks OK, the system will first verify that the new password is not identical to the current password.

This prevents the user from reusing their reset password as the new password.

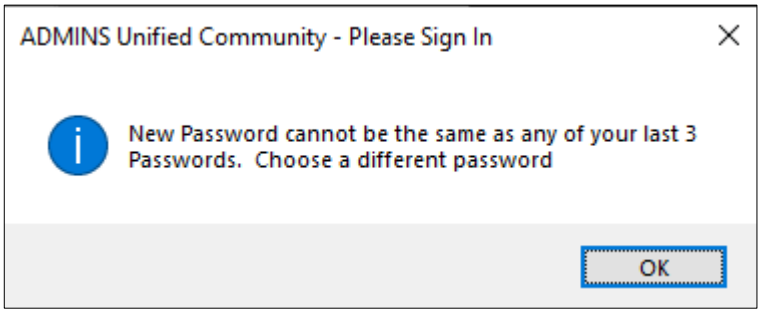
For example, if a password is set to "welcome", the system will not allow "welcome" to be entered as the new password.

A message like this will be displayed:



The system will then compare the new password entered by the user against the last three saved passwords.

If any of these passwords match, the following error message will be displayed.



The user will be brought back to the enter password pop-up again where they can enter a password that has not been used in any of the previous three passwords.

[ADM-AUC-SY-8354]

4 Tracking User Logins [Enhancement]

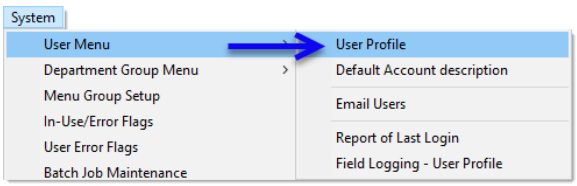
A system administrator reported a suspected login attempt using their AUC credentials.

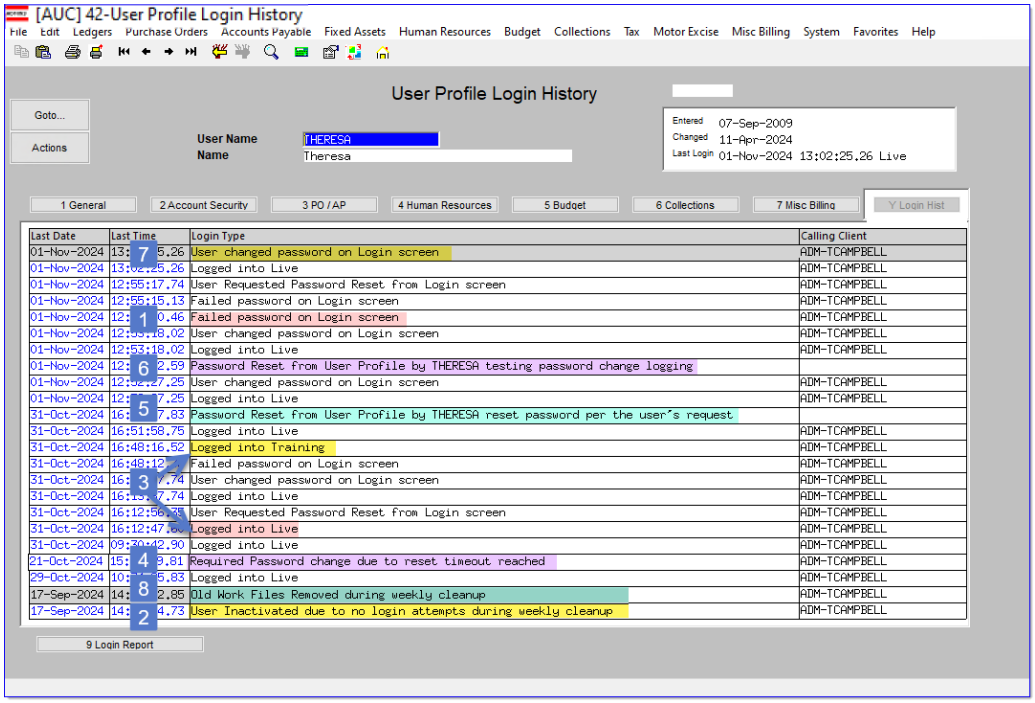
> *"For fear of the worst, I'd like to know if you have an audit log for when someone tries to authenticate, success or fail, from what IP address preferably. Also, when the last time a password change was requested, and completed."*

In response, **ADMINS** now logs more details on the User Profile Login History screen for each user login.

To access the screen from the menu, select:

System ▸ User Menu ▸ User Profile ▸ Y Login Hist





This feature is available only to superusers with a security level of 20+.

The types of details are explained in the sections below that correspond to the numbers in the image. E.G., "1" is explained in section 4.1.1 below.

4.1 Logging More Status Activity

In addition to including the name of the client computer, further details about the type of login activity are provided.

4.1.1 Failed Password/Login Attempt

If a user fails to enter the correct password three times in a row, each failed attempt will show a time and date stamp, along with the client computer name. A message will also display after the 3rd attempt indicating more than three failed attempts.

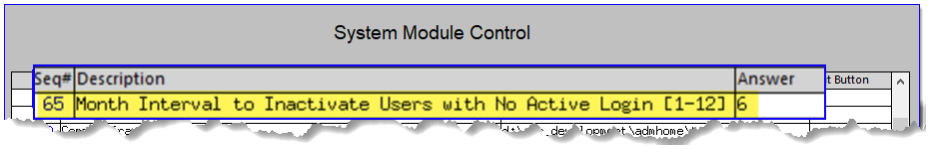
Last Date	Last Time	Login Type
23-Sep-2024	14:47:37.34	Logged into Live
23-Sep-2024	14:18:32.71	User changed password on Login screen
23-Sep-2024	14:18:32.71	Logged into Live
23-Sep-2024	14:18:11.13	Password Reset from User Profile by ANTHEA forgot pwd
23-Sep-2024	14:15:04.00	Logged into Live
23-Sep-2024	14:15:04.00	User changed password on Login screen
23-Sep-2024	14:13:47.28	More than 3 failed password attempts in a row
23-Sep-2024	14:13:43.50	Failed password on Login screen
23-Sep-2024	14:13:40.07	Failed password on Login screen
23-Sep-2024	14:13:33.77	Failed password on Login screen

4.1.2 User Inactivated Due to No Login Attempts

This username was inactivated during a weekly process that compares login history to the value of module control #65. If the number of months since the most recent login exceeds the value of Module Control 65, the username is set to "Inactive" status. It will look like this:

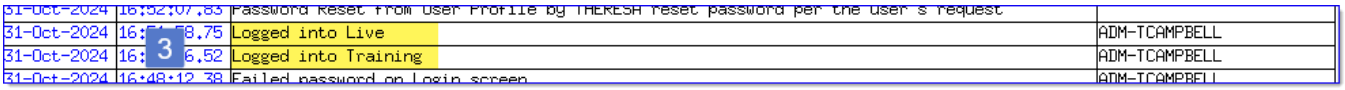
17-Sep-2024	14:	4.73	User Inactivated due to no login attempts during weekly cleanup

The interval on module control #65 is set to six months by default but can be adjusted between 1 and 12 months.



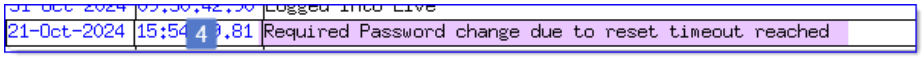
4.1.3 User Successfully Logging into Live or Training

Each login to LIVE or TRAINING will be recorded, with the Date, Time, and Calling Client computer name.

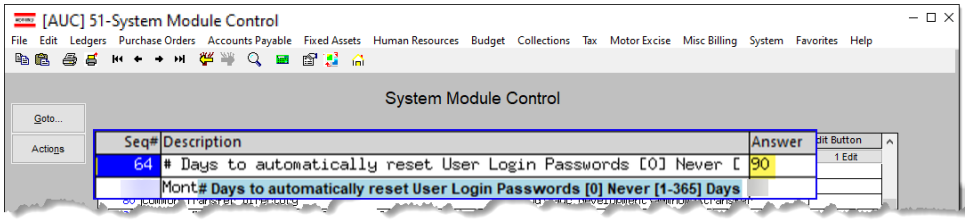


4.1.4 Site Required Password Change

The user was required to change their password because the password age exceeded the number of days specified in Module Control # 64 "Reset Timeout", which mandates a password reset.

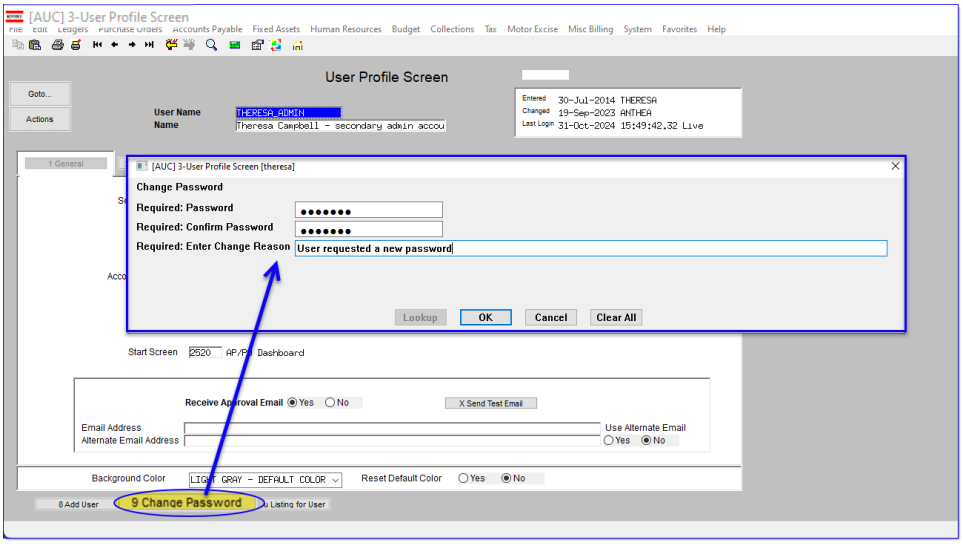


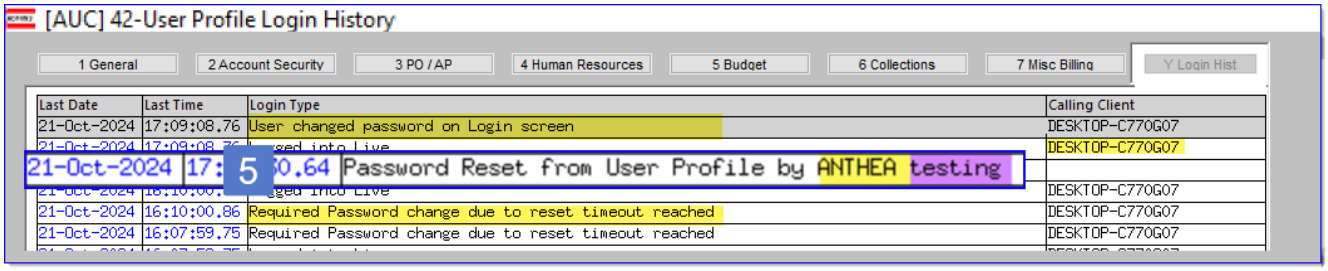
The value of Module Control #64 can be changed only by a superuser or **ADMINS** support.



4.1.5 Password Resets from the User Profile Screen

Password reset from User Profile screen by [username] [change reason]. (Username is included because typically, the change is made by an **ADMINS** support team member *(a MUPDEV* account)* or a site system administrator, not the user.)

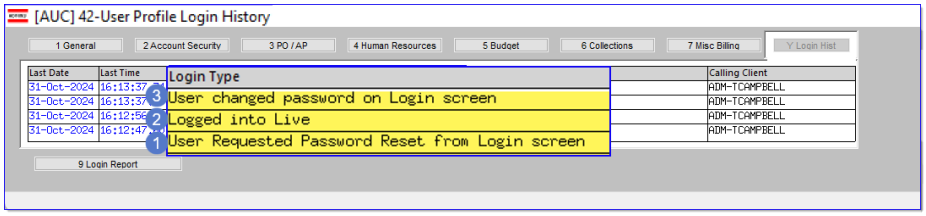




In the example shown the username is “Anthea” and the reason is that she was “testing”.

4.1.6 User Initiated the Password Reset from Their Own Login Screen

When a user requests a password reset from the initial login screen, three entries will be made: 1 indicating the request, 2 showing the user logged into live, and 3 an entry noting the password change on the login screen.



Any user may initiate a reset password request from the login screen. See the release notes in the System Help Reference Library for September 2020 for details.

4.1.7 User Changed Password on Login Screen

This is logged after a password reset is done to verify the user created a new password. This is logged if the user requested a password change or if a system admin reset the password from the user profile, or the user password automatically expired because of module control #64. Any time the user changes their password this is logged.

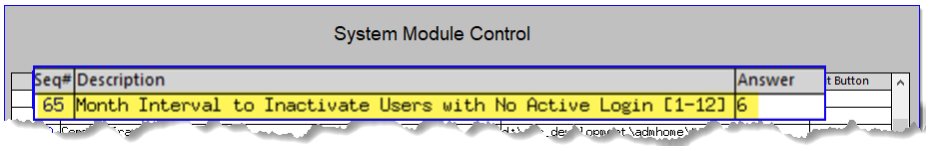
01-Nov-2024	12:53:18.02	User changed password on Login screen	ADM-TCAMPBELL

4.1.8 Old Work Files Removed During Weekly Cleanup

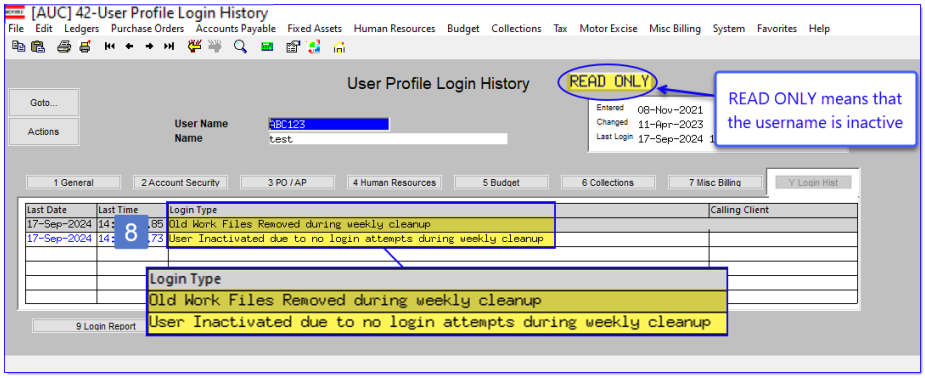
This process will delete user-specific work files for users who have been inactive or have become inactive due to not logging in for six months (or according to the period set by Module Control #65).

Last Date	Last Time	Login Type	Calling Client
17-Sep-2024	14:44:22.85	Old Work Files Removed during weekly cleanup	

The interval on module control #65 is set to six months by default but can be adjusted between 1 and 12 months.

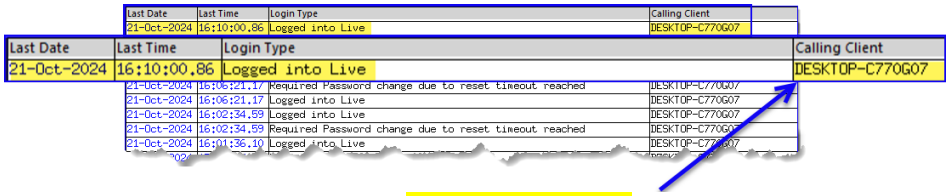


In this example, the weekly maintenance job did two things – it inactivated the user, and also removed old username based work files, based on the "reset value".



4.2 Capture the Name of the Client Computer

When a user logs in, the calling client name (the name of the computer referenced by \\tsclient) will now be displayed. This will provide more information about who attempted to log in as them and reset their password.



In the image, the calling client is "DESKTOP-C770G07". The calling client will be logged for activity from the user login screen (reset password requests, successes, or failures).

Changes made from the User Profile screen by an administrator or MUPDEV account will not show a calling client.

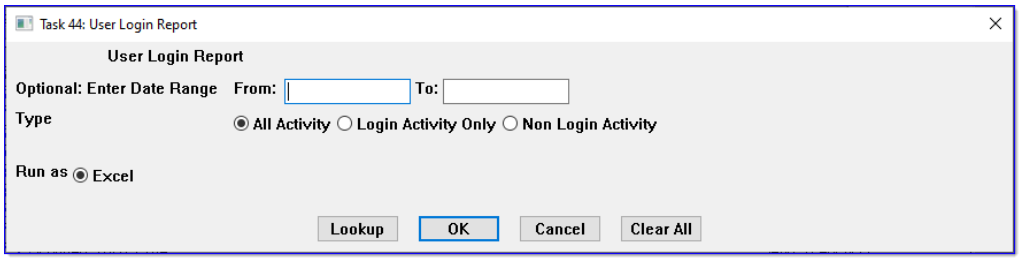
4.3 Reports

There are two reports available for this login history. Both reports are exclusively in Excel format *(because the information would be too small to read on a PDF)*. The layouts of both reports are identical; only the selection criteria differ.

4.3.1 Login Report Button from the Log History Screen

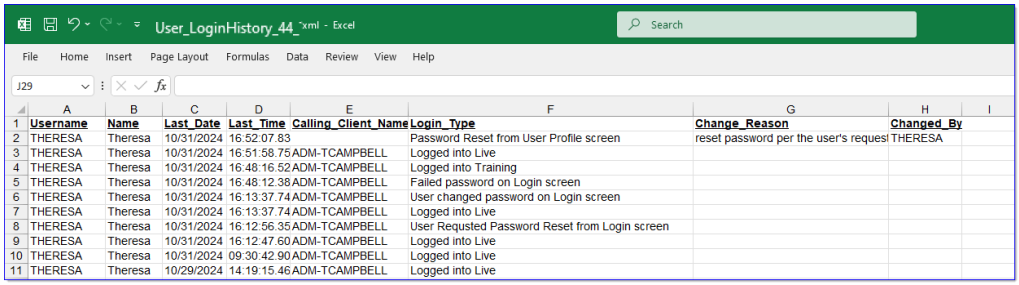
This prompt now includes a radio button to select by the type of activity.

Activities are categorized as either ⊙**Login Activity** (such as logging into live or training) or ⊙**Non-Login Activity** (such as a password reset).



The default setting is ⊙**All Activity**. You may choose to limit the report output within a specific date range by entering the desired dates. If no date range is specified, the report will include all available records for this username.

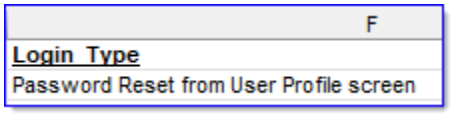
When the report is run from the user profile, only records pertaining to the currently displayed user will be included.



User_LoginHistory_44_*.xml - Excel

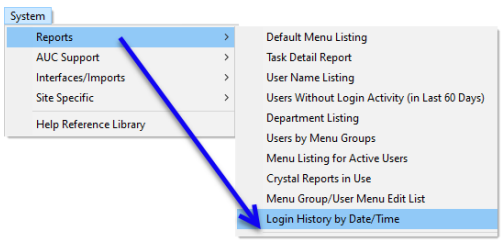
	Username	Name	Last_Date	Last_Time	Calling_Client_Name	Login_Type	Change_Reason	Changed_By
2	THERESA	Theresa	10/31/2024	16:52:07.83		Password Reset from User Profile screen	reset password per the user's request	THERESA
3	THERESA	Theresa	10/31/2024	16:51:58.75	ADM-TCAMPBELL	Logged into Live		
4	THERESA	Theresa	10/31/2024	16:48:16.52	ADM-TCAMPBELL	Logged into Training		
5	THERESA	Theresa	10/31/2024	16:48:12.38	ADM-TCAMPBELL	Failed password on Login screen		
6	THERESA	Theresa	10/31/2024	16:13:37.74	ADM-TCAMPBELL	User changed password on Login screen		
7	THERESA	Theresa	10/31/2024	16:13:37.74	ADM-TCAMPBELL	Logged into Live		
8	THERESA	Theresa	10/31/2024	16:12:56.35	ADM-TCAMPBELL	User Requsted Password Reset from Login screen		
9	THERESA	Theresa	10/31/2024	16:12:47.60	ADM-TCAMPBELL	Logged into Live		
10	THERESA	Theresa	10/31/2024	09:30:42.90	ADM-TCAMPBELL	Logged into Live		
11	THERESA	Theresa	10/29/2024	14:19:15.46	ADM-TCAMPBELL	Logged into Live		

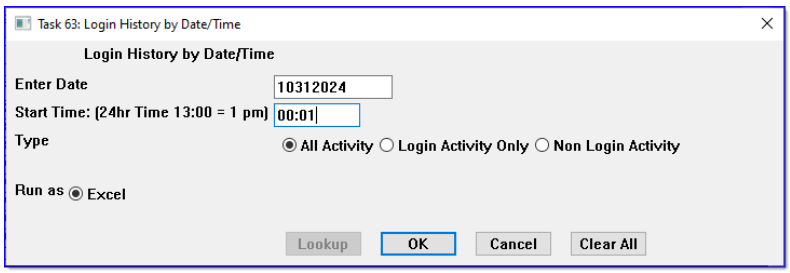
The above report was run with ⊙ **All Activity** selected, so the list includes activity such as Password resets that were made from the user profile table.



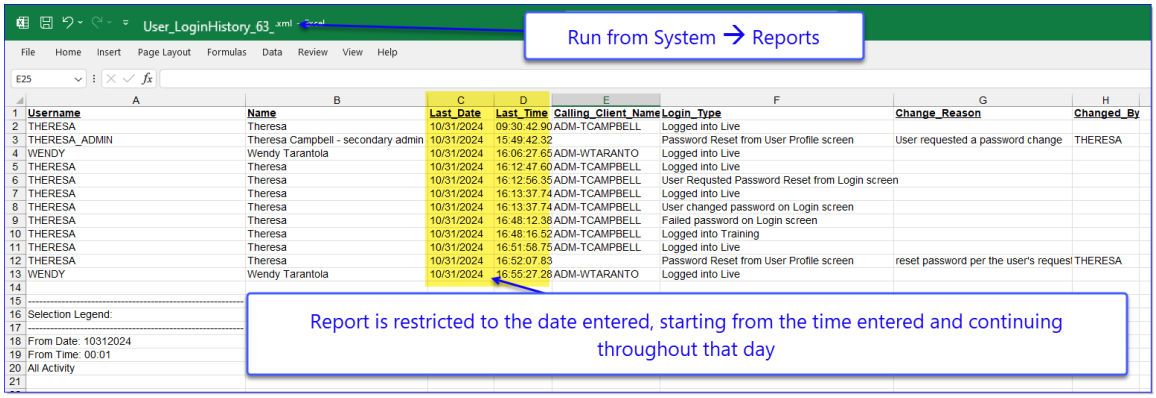
	F
Login_Type	
Password Reset from User Profile screen	

4.3.2 Report on the System Menu





This prompt now asks for the activity type to report. The output is limited to activity on the specified date, starting from the entered time and covering the rest of that day. Since the start time was entered as 00:01, all activity from 31 October 2024 is listed.



4.4 Changes to User Profile

When resetting a password from the user profile screen, you must now provide a reason. Possible reasons include:

1. The user forgot their password, and it's easier for MUPDEV to change it than to have them click the reset button.
2. The user has no email address set up on their profile.
3. Other reasons...

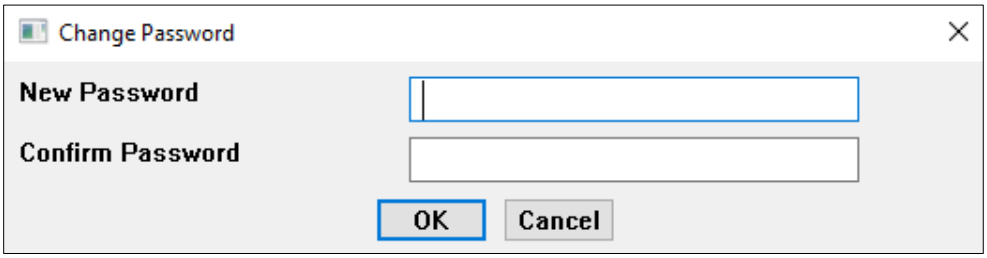


Figure 5 Before the software update, there was nowhere to enter a "reason" on the prompt

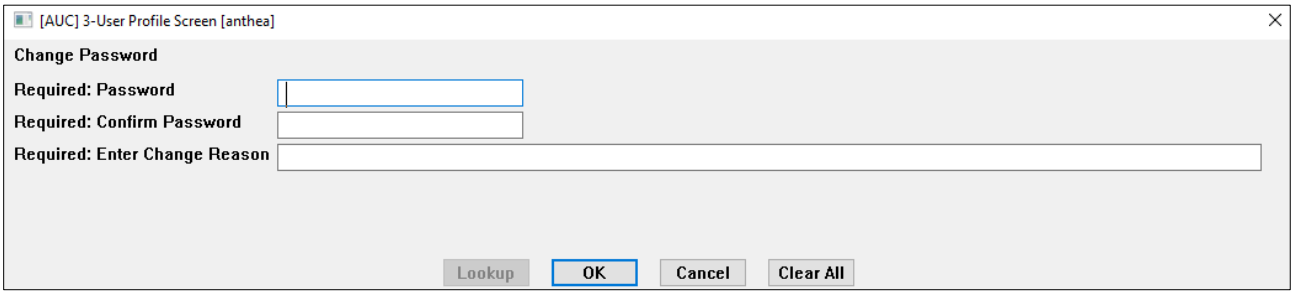


Figure 6 Since the software update, the prompt requires a reason for the password change

[ADM-AUC-SY-8349]

5 Help Reference Library

Updated the Help Reference Libraries and ADMINS.com with new or revised content.

5.1 Accounts Payable

Enter Vouchers/Process Payments	AP-145 Preventing Duplicate Payments	[Updated]

5.2 Budget

Processing	BU-110 Budget Processing	[Updated]

5.3 Miscellaneous Billing

Site Specific	MB-610 HVMA Monthly Miscellaneous Billing Reconciliation	[Updated]
	MB-630 HVMA Customer Maintenance	[New]
	MB-632 HVMA Set Up Tables for Condominium Transactions	[New]
	MB-635 HVMA Condominium Leases	[New]
	MB-637 HVMA Condominium ReSales	[New]
	MB-639 HVMA Condominium Reports	[New]
	MB-645 HVMA Condominium Bank Questionnaires	[New]
	MB-650 HVMA HOA Billing	[Updated]
	MB-655-HVMA Generate EFT File Instructions	[New]
	MB-670 HVMA Apply Pre-Payments to Outstanding Invoices	[Updated]
	MB-690 HVMA Set Up Tables & Forms *(for billing)*	[Updated]

5.4 Revenue Collections

Treasury Receipts	RC-1320 Treasury Receipts	[Updated]
	RC-1355 Supplemental Appropriations JE from a TR	[Updated]

5.5 System

System	SY-101 Site Editable Module Control Sequence Values	[New]

5.6 New Content on ADMINS.com

Create New Voucher from Posted Voucher Video (3:08) (video)
User Account Security Inquiry Screen (2:38) (video)