PAA Password Reset

CSR PasswordReset should be used to unlock accounts by providing a temporary passwords for Agent and Employer **PAA's ONLY.**

Resetting and assigning temporary passwords is something that requires a high level of security. Please be sure to follow all steps and always authenticate the user you are speaking with. If authentication of the user is not performed before resetting the password we run the risk of losing access to these tools.

The first step in resetting the password for a user is to confirm if they are the PAA or a Secondary user. We can do this by searching the agent or group ID in **IT Security Management Screens**. Instructions on how to search within this tool can be found in IT Security Management Screens.

NOTE: Users authenticated as a secondary user will need to contact their PAA for password assistance. We CAN provide the PAA name to a secondary user, reach out to the PAA to help them reset a secondary user password and offer to provide instructions on resetting a secondary user.

Before resetting a password be sure to authenticate the web user by verifying the below information.

Employer PAA

Authenticate the user Commercial Agent and Benefit Administrator

To assist the user with online access or navigation the additional requirements below need to be fulfilled

- User ID
- Confirm the user ID is for the user you are speaking with in IT Security Management Screens ○ Secured Logons Administration Reference

Agent/Broker PAA

Authenticate the user Commercial Agent and Benefit Administrator

To assist the user with online access or navigation the additional requirements below need to be fulfilled

- User ID
- Confirm the user ID is for the user you are speaking with in IT Security Management Screens.
    - ○ Secured Logons Administration Reference

Password Reset Process

Confirm if the user **is locked out** of the account **or** has forgotten their log on information and **is not yet locked out.**

1. **If the user IS locked out:**
    a. Confirm they know the answer to their security question.
        i. Instructions on verifying security question/answer can be found here:
        ii. Secured Logons Administration 7.0 - **Reset Secret Prompt**
        NOTE: When verifying the security question/response we do not provide hints as to what the answer is. Often times the user is just entering the security answer in the incorrect format. Please review the above document for additional instructions.
        iii. If the user is unable to verify their Security answer a Service Now incident is created and a call is initiated to Access Management to revoke the account.
        iv. An incident is required whenever a call is initiated to Access Management. Please refer to the appropriate document below for additional information on submitting incidents to security.
            1. Submitting Changes for Employer Secured Logons Applications
            2. Submitting Changes for Agency and Broker Secured Logons Applications

NOTE: Performing the revoke to allow the user to set up a new security question on the first call is ideal. This will ensure that the next time the user needs to reset their password they can do so successfully and they don't have to call in again. (If the user does not wish to be transferred to Access Management set the expectation that they will need to call in again should they have additional access issues in the future)

    b. **After the user has provided the correct security question**, unlock the account using CSR Password Reset. Provide the temporary password to the user and confirm they are able to follow the steps to reset their password.
    NOTE: If the user **resets their password through the path of entering their security answer AFTER a CSR Password reset has been performed**; they will be required to reset their password twice. It is encouraged that you provide them with a temporary password after they have confirmed the security answer.
    c. Confirm the user is able to access their account successfully.

2. **If the user is NOT locked out:**
    a. Confirm they know the answer to their security question. Instructions on verifying security question/answer can be found here:
        i. Secured Logons Administration 7.0 - **Reset Secret Prompt**
        NOTE: When verifying the security question/response we do not provide hints as to what the answer is. Often times the user is just entering the security answer in the incorrect format. Please review the above document for additional instructions.
    b. If the user **is able to confirm the security answer** walk the user through the steps on the sign in screen to reset password. Enter the group ID or SAN and answer to the security question. Confirm the user is able to access the account successfully.
    c. If the **user is unable to verify their Security answer** a Service Now incident is created and a call is initiated to Access Management to revoke the account.

i. An incident is required whenever a call is initiated to Access Management. Please refer to the appropriate document below for additional information on submitting incidents to security.
   1. Submitting Changes for Employer Secured Logons Applications
   2. Submitting Changes for Agency and Broker Secured Logons Applications

NOTE: Performing the revoke to allow the user to set up a new security question on the first call is ideal. This will ensure that the next time the user needs to reset their password they can do so successfully and they don't have to call in again. (If the user does not wish to be transferred to Access Management set the expectation that they will need to call in again should they have additional access issues in the future)

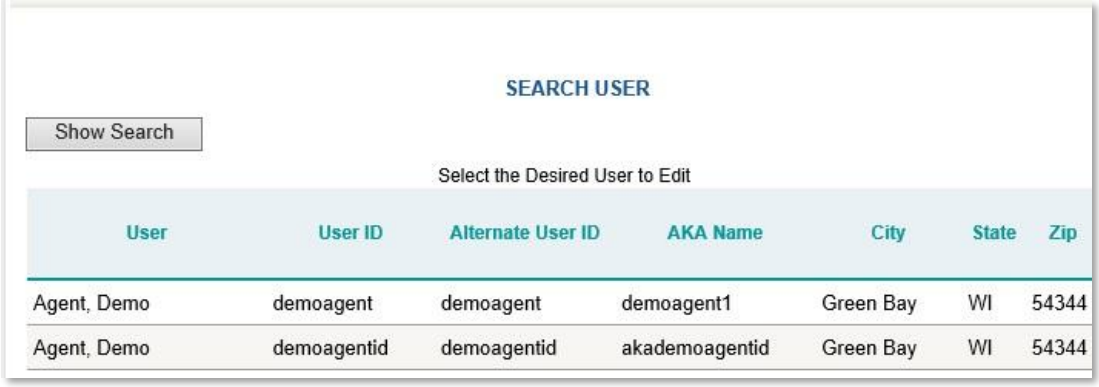
3. Since the transition to Unified Logons in May 2021, Access Management is **no longer able to reset the security question**. If the user is unable to verify their security answer, Access Management is required to revoke the account so the user can create a new profile and select a new security question.

To reset the password for an authenticated PAA go to **HSS** and select CSR PasswordReset.

Select field **User ID/Alternate User ID** and enter the User ID that was provided to you by the web user.

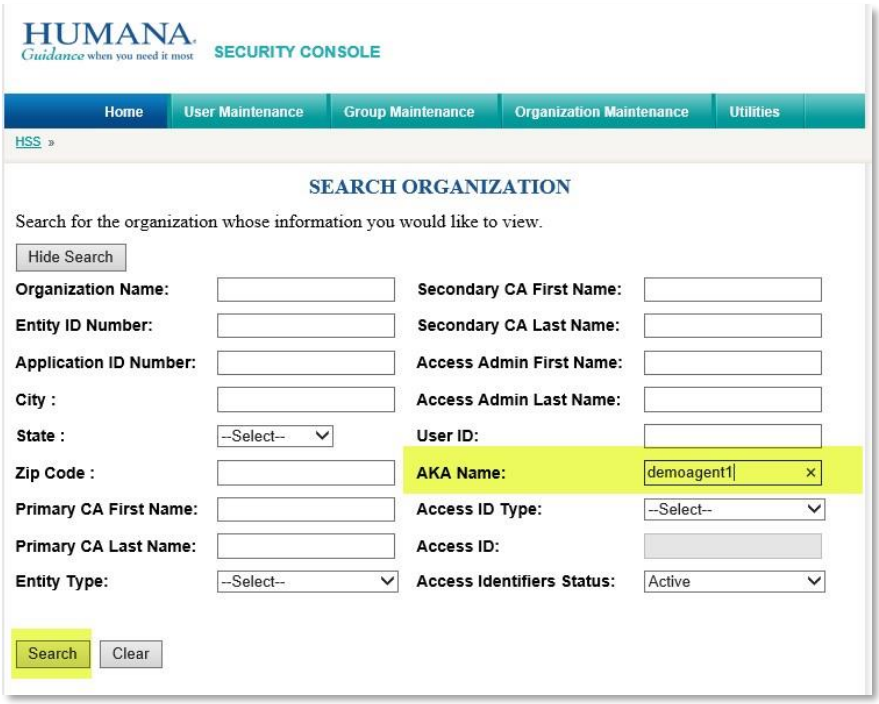
The search user screen will display the web apps that are tied to a user ID similar to the one that was entered. **Please ensure you select the correct user associated with the User ID and confirm that is the person you are speaking with.**
NOTE: We do not reset passwords for anyone other than who the username belongs to.

If you are unsure if that username is tied to the agent or group account you are speaking about, you can verify by going to IT Security Management Screens and search by AKA name.



To search the AKA name in IT Security Management Screens:

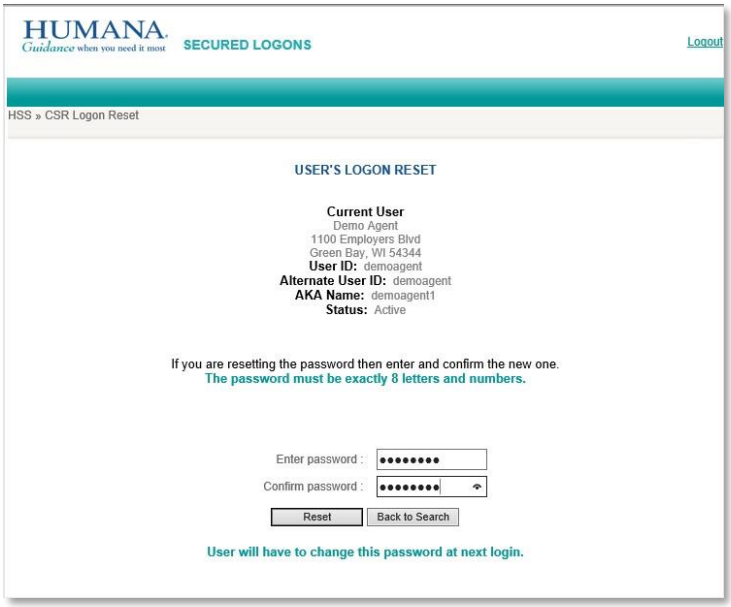
- Access IT security Management Screens in HSS.
- Select App/Org/Admin Lookup Menu (Bus Contact).
- Select Display Current Organization Information.
- Enter the AKA Name that was found on the Search User screen and Search.



After searching the AKA confirm:

- The SL App # matches the App ID that came up when searching the group or agent ID
- Do the identifiers on the app match what the caller provided to authenticate? (Group ID or Agent SAN)
- The caller is listed as a web users ○ If the caller is a secondary user direct them back to the PAA for password assistance. Offer to reach out to the PAA to assist with secondary password resets.

After you have verified the username is for the PAA you are speaking with enter a temporary password that is exactly 8 characters long. Select Reset. This will reset the number of attempts as well as the password for the account. Provide the user with the temporary password and confirm they are able to log in using the password provided.



If the password reset was not successful follow the steps below:

Password reset failure

- If you receive an error when trying to reset a PW:
- Create an incident in ServiceNow and assign to SRE_IAM_Core previously SLPNR
- Summary use **"Employer/Agent user unable to reset PW"** ○ Please refer to ServiceNow Intro for additional instructions on submitting incidents
- User ID
- SL app ID
- Organization name on SL App
- Description of the error (screen shots)
- Leave cases open and follow up with users once IT resolves.

If after resetting the password and confirming the username for the user they are receiving an error on Humana.com, "Username and Password does not match our records." **Confirm the user is re-entering the username and password in the applicable fields**. If the user has a saved username in this field this may prevent them from being able to log in to their account.